

**Official Transcript of Proceedings**  
**NUCLEAR REGULATORY COMMISSION**

Title:                   Advisory Committee on Reactor  
                              Safeguards Design Acceptance Criteria  
                              Subcommittee

Docket Number:       (n/a)

Location:               Rockville, Maryland

Date:                    Thursday, October 21, 2010

Work Order No.:       NRC-504

Pages 1-219

NEAL R. GROSS AND CO., INC.  
Court Reporters and Transcribers  
1323 Rhode Island Avenue, N.W.  
Washington, D.C. 20005  
(202) 234-4433

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, as reported herein, is a record of the discussions recorded at the meeting.

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 UNITED STATES OF AMERICA

2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5 (ACRS)

6 + + + + +

7 DESIGN ACCEPTANCE CRITERIA (DAC) SUBCOMMITTEE

8 + + + + +

9 THURSDAY, OCTOBER 21, 2010

10 + + + + +

11 ROCKVILLE, MARYLAND

12 The Advisory Committee met, at the Nuclear  
13 Regulatory Commission, Two White Flint North, Room  
14 T2B1, 11545 Rockville Pike, Rockville, Maryland, at  
15 1:00 p.m., Dennis C. Bley, Chairman, presiding.

16 SUBCOMMITTEE MEMBERS:

17 DENNIS C. BLEY, Chairman

18 SAID ABDEL-KHALIK, Member

19 J. SAM ARMIJO, Member

20 MARIO V. BONACA, Member

21 CHARLES H. BROWN, Member

22 JOY REMPE, Member

23 MICHAEL T. RYAN, Member

24 WILLIAM J. SHACK, Member (via telephone)

25 JOHN W. STETKAR, Member

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

## C-O-N-T-E-N-T-S

1		
2	<i>Call to Order, Opening Remarks and Objectives</i>	<b>4</b>
3	<i>Dennis Bley, Chairman</i>	
4	<i>Statement by Laura Dudes</i>	<b>7</b>
5	<i>Deputy Director</i>	
6	<i>Division of Engineering</i>	
7	<i>Office of New Reactors</i>	
8	<i>AP1000 Example</i>	<b>12</b>
9	<i>Terry Jackson</i>	<b>12</b>
10	<i>Chief, Instrumentation, Controls</i>	
11	<i>and Electrical Engineering Branch 1</i>	
12	<i>William Roggenbrodt</i>	
13	<i>Technical Lead for the I&amp;C Review</i>	
14	<i>for the AP1000</i>	
15	<i>Dan Santos</i>	
16	<i>Senior-Level Advisor</i>	
17	<i>ESBWR Example</i>	<b>88</b>
18	<i>Ian Jung</i>	<b>88</b>
19	<i>Chief, Instrumentation, Controls</i>	
20	<i>and Electrical Engineering Branch 2</i>	
21	<i>Kimberly Corp</i>	<b>92</b>
22	<i>Dinesh Taneja</i>	<b>95</b>
23		
24		
25		

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

<i>Inspection Activities</i>	<i>149</i>
<i>Tom Fredette</i>	<i>149</i>
<i>Division of Construction Inspection and Operational Programs Construction Inspection Programs Branch</i>	
<i>Industry Remarks</i>	<i>194</i>
<i>Kimberly Keithline</i>	
<i>NEI</i>	
<i>Members' Closing Comments</i>	<i>203</i>
<i>Staff's Closing Comments</i>	<i>215</i>

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

*P-R-O-C-E-E-D-I-N-G-S*

*1:00 p.m.*

*CHAIRMAN BLEY: The meeting will now come to order.*

*This is a meeting of the Future Plant Design Subcommittee. I'm Dennis Bley, Chairman of the Subcommittee.*

*ACRS members in attendance are Charlie Brown, John Stetkar, Said Abdel-Khalik. Bill Shack is listening in on a bridge line. Joy Rempe is here. Jack Sieber is due here, but he is not here yet. Mario Bonaca and Mike Ryan.*

*Did I miss anybody? I don't think so.*

*Oh, Sam, Sam Armijo.*

*Christina Antonescu of the NRC staff is our Designated Federal Official for this meeting.*

*The purpose of this meeting is to discuss the ongoing issues related to closure of the Design Acceptance Criteria, DAC, for new reactors. The focus of this meeting is going to be on digital I&C DAC, and it is going to be on the technical issues. We want to get through some examples. So we want to not spend the time on process here we have spent on other meetings.*

*Specifically, the staff plans to discuss*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 two ITAAC, Inspection Tests Analysis and Acceptance  
2 Criteria, that were considered back at the initiation  
3 of the AP1000 amendment review, and one DAC and a  
4 subsequent ITAAC that were reviewed during the design  
5 certification review of ESBWR.

6 As background, the Committee issued a  
7 letter to Chairman Jaczko, dated 9 August 2010, that  
8 provided the Committee's view on staff's activities on  
9 closure of DAC for new reactors. The letter provided  
10 the following conclusions and recommendations:

11 DAC closure requires expertise, judgment,  
12 and interpretation. It should be performed by NRC  
13 staff experts with an independent assessment by ACRS.

14 And two, it is preferable that all DAC be  
15 resolved no later than the combined operating license  
16 stage. However, whether resolved as part of COL  
17 process or post-COL, proper closure of DAC requires a  
18 consistent scope and depth of evaluation, in  
19 accordance with the first recommendation.

20 The Subcommittee will gather information,  
21 analyze relevant issues and facts, and formulate  
22 proposed positions and actions, as appropriate, for  
23 deliberation by the full Committee.

24 The rules for participation at today's  
25 meeting have been announced as part of the notice of

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 this meeting, previously published in *The Federal*  
2 *Register* on October 4th, 2010.

3 We have received no written comments.  
4 However, we have received a request for time to make  
5 an oral statement and presentation from Ms. Kimberly  
6 Keithline of Nuclear Energy Institute, NEI, as a  
7 member of the public, regarding today's meeting.

8 We also have a number of people listening  
9 into the discussion on the bridge line. They include  
10 Mr. Keith Fletcher, reporter for Nuclear New Build  
11 Monitor, and a number of representatives from a  
12 variety of firms, including GE Hitachi Nuclear Energy,  
13 Dominion Resources Services, Nuclear Plant  
14 Development, Southern Company, Mitsubishi Nuclear  
15 Energy Systems, PSEG Nuclear Development.

16 And I guess I would ask, are there any  
17 others listening in on the bridge line? If so, please  
18 identify yourselves.

19 (No response.)

20 I guess that's it.

21 To preclude interruption of the meeting,  
22 the phone line will be placed in the listen-in mode  
23 during the discussions and presentations and during  
24 Committee discussions.

25 Member Dr. Shack is on a separate bridge

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 line and will be able to participate in the  
2 discussions.

3 A transcript of the meeting is being kept  
4 and will be made available, as stated in The Federal  
5 Register notice. Therefore, we request that  
6 participants in this meeting use the microphones  
7 located throughout the meeting room when addressing  
8 the Subcommittee. Participants should, first,  
9 identify themselves and speak with sufficient clarity  
10 and volume, so that they may be readily heard.

11 We will now proceed with the meeting. I  
12 guess, first, I will turn it over to Laura Dudes from  
13 staff.

14 MS. DUDES: Thank you.

15 I am Larry Dudes. I am the Deputy  
16 Director for the Division of Engineering in the Office  
17 of New Reactors.

18 First, I would like to thank the Committee  
19 for this important opportunity and the time that you  
20 are giving us today, so we can focus on the safety of  
21 the digital I&C system.

22 The purpose of today's meeting is to seek  
23 feedback from the ACRS and arrive at a common  
24 understanding of concerns associated with the  
25 resolution of Design Acceptance Criteria. It is also

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for us to have some time to present the methods the  
2 staff uses to review the digital I&C system and arrive  
3 at a safety finding.

4 And lastly, we would like to present the  
5 method and plans that the staff is developing to  
6 resolve Design Acceptance Criteria associated with the  
7 digital I&C Design Acceptance Criteria.

8 Next slide.

9 Expected outcomes. I would say that I  
10 think the success for today's meeting is obviously we  
11 want to be proactive in giving you as much information  
12 as we have in terms of how we perform our review, the  
13 level of detail we go to over a very significant two-  
14 to-five-year period of review, anywhere from 5 to 10  
15 thousand hours of staff review, and the scope of that  
16 review.

17 At the same time, the staff wants to be  
18 cognizant and listen to the Committee's concerns  
19 associated with this review, associated with our  
20 safety findings, and concerns associated with the  
21 Design Acceptance Criteria generically as well as how  
22 we plan to resolve them.

23 Next slide.

24 I believe, Dennis, you had gone through  
25 the letters and the recent developments. So I think

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we are all aware of where we are at in terms of  
2 communication.

3 So we will go to the next slide.

4 This afternoon staff plans to cover two  
5 examples, very interesting examples. One is for the  
6 AP1000 Design Center. The second is for the ESBWR  
7 Design Center.

8 It is interesting to note that, as the  
9 staff goes through the AP1000 Design Center, this  
10 applicant has chosen to resolve the necessary  
11 information associated with a previous Design  
12 Acceptance Criteria in a previous revision to the  
13 design. They have done so during or via a license  
14 amendment. So they are going to talk through how the  
15 NRC headquarters staff performed a licensing review to  
16 resolve and eliminate a specific Design Acceptance  
17 Criteria in that Design Center.

18 For the ESBWR example, the staff still is  
19 going to continue to present the scope and level of  
20 depth of the review they performed associated with the  
21 ESBWR design and the DAC that they reviewed which  
22 support their safety finding.

23 Next slide.

24 We're all about the visuals today. I  
25 think you all notice we have carted down our hard

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *copies of all our technical reports as well as the DCD*  
2 *Chapter 7 that we review. I think we are trying to*  
3 *continue to emphasize the point that these reviews*  
4 *take anywhere from two to five years, anywhere from*  
5 *5,000 to 10,000 to 15,000 hours, depending on the*  
6 *complexity of the design.*

7 *So this slide is really just telling you*  
8 *that the example associated with our discussion today*  
9 *is a slice of the entire scope and review of a broader*  
10 *systematic review of the entire digital I&C system*  
11 *included in Chapter 7 of the design documents.*

12 *Next slide.*

13 *I think this is a similar depiction,*  
14 *again, indicating that the example for the ESBWR that*  
15 *we are going to review today, again, is just one*  
16 *aspect of a very complex review.*

17 *Next slide.*

18 *So this afternoon the staff is going to go*  
19 *through the DAC resolution method, scope, and depth of*  
20 *evaluation. We are going to describe the safety*  
21 *issues. We are going to describe associated*  
22 *regulatory requirements that the staff used, verified,*  
23 *which satisfied the safety issue. We will provide a*  
24 *summary and relevant examples of information submitted*  
25 *by the applicant. We will give a brief explanation of*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the method used by the staff for its review, an  
2 explanation as to why it was acceptable to have a  
3 particular DAC in a design document. We will also  
4 provide an assessment of the quality of the Design  
5 Acceptance Criteria itself.

6 Then, we also have members from the  
7 Division of Construction Inspection Program here today  
8 who will be presenting our plans for how we plan to  
9 resolve DAC in the inspection phase.

10 I do want to point out that there is  
11 limited space up at the front of the table, but during  
12 the course of the day you will have members from the  
13 Division of Construction Inspection Program, technical  
14 staff from the Division of Engineering staff, senior  
15 licensing project managers, and advisors from our  
16 Licensing Division. So the collective group of people  
17 presenting today do represent NRO's team effort  
18 associated with the review of digital I&C, the review  
19 and acceptance of the Design Acceptance Criteria, and  
20 then the supporting roles in terms of how we will  
21 resolve the Design Acceptance Criteria in the future.

22 So, with that, I would like to turn it  
23 over to the staff, who have given you a rather large  
24 package with some examples. I know they would like to  
25 get into the details.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1            *CHAIRMAN BLEY: Before you begin, I should*  
2 *have mentioned at the beginning it was pointed out*  
3 *that it could be possible we would have to close the*  
4 *meeting to talk about some particular issues. If that*  
5 *happens, we will reserve those until the late end of*  
6 *the meeting and do it at that time.*

7            *ME. JACKSON: All right. Thank you. My*  
8 *name is Terry Jackson. I'm the Chief of*  
9 *Instrumentation, Controls, and Electrical Engineering*  
10 *Branch 1, and I have with me Bill Roggenbrodt. He was*  
11 *the technical lead for the I&C review for the AP1000,*  
12 *and as well Dan Santos is our senior-level advisor.*

13            *Go ahead, Dan, to the next slide.*

14            *So what we want to do in the AP1000*  
15 *presentation is we want to talk about the level of*  
16 *effort and depth of review that we used to resolve*  
17 *Design Acceptance Criteria in the AP1000. And we will*  
18 *talk a little bit about the tools that we used, which*  
19 *include the requirements, guidance, documents, and*  
20 *resources used to resolve that DAC.*

21            *What we hope to do is correlate the staff*  
22 *efforts used in this example to future DAC resolution*  
23 *efforts, and our hope is that there will be a better*  
24 *understanding of the scope of the staff effort and*  
25 *review for DAC resolution and the tools and resources*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that we use to do that.

2 Okay, next slide.

3 So this is just outlining some of the  
4 things that we plan to talk about. First, I will give  
5 a little bit of background about the AP1000 timberline  
6 because, as Laura had mentioned, there are several  
7 activities that occurred over several years with  
8 regard to the AP1000, including its original  
9 certification, as well as the amendment efforts.

10 Then, we will get into the AP1000 DAC  
11 example and address these particular items which are  
12 on this slide.

13 Then, finally, we will talk about future  
14 activities with regard to AP1000 and the remaining DAC  
15 in that design.

16 So, to begin with the timberline, in March  
17 of 2002, Westinghouse submitted the design  
18 certification application for the AP1000. So the  
19 staff reviewed that design and approved it. ACRS  
20 reviewed it, and the Commission certified that design  
21 in January of 2006.

22 A couple of months after that, then  
23 Westinghouse determined that the planning activities  
24 phase of the software development life cycle for the  
25 Protection and Safety Monitoring System was complete.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1       *Now the Protection and Safety Monitoring System is*  
2       *the primary protection system for the AP1000.*

3               *Then Westinghouse began interacting with*  
4       *the staff in 2006, beginning with the NRO staff before*  
5       *NRO was created, and then later with the NRO staff.*  
6       *And in October of 2008, the staff began the acceptance*  
7       *review for the AP1000 Design Certification Amendment.*

8               *Next slide.*

9               *So this slide here and the next slide,*  
10       *what I am presenting is what were considered the*  
11       *Design Acceptance Criteria within the AP1000 from the*  
12       *certified design.*

13               *So, the first one has to do with the*  
14       *Diverse Actuation System. And this ITAAC is Item 4 in*  
15       *Tier 1, Table 2.5.1-4. The first two life cycle*  
16       *phases for this ITAAC or for the DAS software*  
17       *development process were the Design Acceptance*  
18       *Criteria portion of the ITAAC.*

19               *And Westinghouse uses different*  
20       *terminology for their software development life cycles*  
21       *as compared to the staff's Standard Review Plan. We*  
22       *define the design requirements phase as planning*  
23       *phase, and we define the system definition phase as*  
24       *the requirements specification stage.*

25               *Okay, next slide.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           So, the second Design Acceptance Criteria  
2 area was with the Protection Safety Monitoring System,  
3 or PMS. That ITAAC is similar to the one that was for  
4 the Diverse Actuation System.

5           So, continuing on with the timberline --

6           MEMBER BROWN: Back up, you said 11 was  
7 also the Diverse -- I thought you said that was the  
8 DMZ as opposed to the Diverse Actuation System.  
9 Either that, or I missed your link.

10          ME. JACKSON: Yes, in this one, this is  
11 the Design Acceptance Criteria associated with the  
12 DMZ, and it is Item 11 of Tier 1, Table 2.5.2-8, and  
13 the previous one was for the Diverse Actuation System.

14          MEMBER BROWN: Okay. All right. Okay. I  
15 thought you were mixing them. Excuse me.

16          ME. JACKSON: So, beginning in February  
17 2008, my staff was heavily engaged with the Design  
18 Certification Amendment review. In April of 2008, we  
19 began reviewing proprietary Westinghouse documents  
20 related to the planning activities.

21                So these -- and correct me if I'm wrong,  
22 Bill -- but these are the procedures that Westinghouse  
23 will use at their facility to guide their software  
24 development process.

25          ME. ROGGENBRODT: That's correct, and they

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 wouldn't be something we would need to see in  
2 licensing space.

3 ME. JACKSON: Right. So these are  
4 detailed procedures that they actually use, their  
5 development people use.

6 Throughout the review, we generated 63  
7 requests for additional information originally, and  
8 that was in May of 2008. And Westinghouse provided --

9 MEMBER SHACK: Can I ask you a question?  
10 This is Bill Shack.

11 ME. JACKSON: Sure.

12 MEMBER SHACK: If we are looking at this  
13 as the resolution of a DAC, I thought that was to be  
14 done on an inspection process. These 63 RAIs, is that  
15 part of the inspection?

16 ME. JACKSON: That was part of the overall  
17 amendment review. So I was just giving background for  
18 all the activities associated with it. And later on  
19 in the slides, we will narrow it down to a very  
20 specific example.

21 MS. DUDES: And let me just clarify. This  
22 is Laura Dudes again. There are three ways to resolve  
23 a Design Acceptance Criteria, when the Design  
24 Acceptance Criteria are captured in a Design Control  
25 Document, in a DCD.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           An applicant can choose to submit a  
2           licensing amendment, and we will actually amend that  
3           Design Certification and then go through rulemaking a  
4           second time. So, Westinghouse, for this particular  
5           case, chose to submit an amendment to their DCD which  
6           the staff is reviewing, and then we will go through a  
7           second rulemaking to incorporate all of the changes,  
8           and there will be a new Design Certification.

9           The other avenue to resolve a DAC is --

10          CHAIRMAN BLEY: I know you are going to  
11          get to them. Can I ask a question about that one?

12          It appears to me, when they do that, they  
13          don't really submit the amendment and say they are  
14          resolving DAC No. 32. They submit an amendment that  
15          doesn't include the DAC, but includes design  
16          information.

17          MS. DUDES: Correct.

18          CHAIRMAN BLEY: That's right?

19          MS. DUDES: That's correct.

20          CHAIRMAN BLEY: Okay.

21          MS. DUDES: Yes. And then, the other  
22          mechanisms are you can either do it during -- a COL  
23          applicant could provide that supplemental information  
24          and then remove the DAC from their license.

25          Then, the final, which is just as viable

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of a method to resolve DAC, is the DAC remains in the  
2 DCD. The COL is issued, and then there is an  
3 inspection activity, because DAC are ITAAC, and  
4 there's an in-depth inspection activity, which we will  
5 discuss later, which will also resolve that.

6 So, in this particular case --

7 MEMBER SHACK: Okay. Well, I guess my  
8 point is that I expect the depth and scope of the  
9 review to be the same, no matter how you resolve it.

10 ME. JACKSON: Yes, I think we will get to  
11 that.

12 MEMBER SHACK: I would like to know where  
13 the equivalent of these RAIs will come into that last  
14 one, if you can sort of think ahead when you're  
15 discussing that.

16 ME. JACKSON: Okay. Yes, as we go through  
17 our slides. Right now, we are just giving more of the  
18 background, and those 63 RAIs were associated with the  
19 entire amendment for I&C-related. The DAC were a  
20 portion of the amendment. As we go through the  
21 slides, we will narrow it down, and then we will focus  
22 on what part those RAIs played in it and the other  
23 efforts, including our audits.

24 MEMBER BROWN: Let me break that down just  
25 a little bit more, if you don't mind. They submitted

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the initial DCD license amendment. And that's to  
2 eliminate, regardless of how they subtracted them off  
3 the list of DAC, that's what the purpose was? You  
4 reviewed it. You did the RAI routine. You went  
5 through all that stuff. You come to the conclusion  
6 that's valid. Then that's one method that Laura just  
7 mentioned.

8 The second method was COL, the licensee.  
9 After that, you all give them the certification.  
10 Could decide to remove DAC as well?

11 MS. DUDES: Correct.

12 MEMBER BROWN: And I presume that the  
13 licensee would then have to go through the same  
14 amendment request process where -- let me finish --  
15 where you would get the RAIs in? This is if  
16 Westinghouse hadn't done that and it was put off until  
17 the COL stage.

18 ME. JACKSON: Okay.

19 MEMBER BROWN: Okay? Now the COL decides  
20 he wants to eliminate DAC. So they would then submit  
21 an amendment to eliminate the DAC with the requisite  
22 design information incorporated in a revision of their  
23 own to the DCD? And that would, then, be reviewed by  
24 staff, NRC, in the same level of detail?

25 I'm trying to piggyback on Bill Shack's

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 comment. So, at that point, that's where you would  
2 get the same level of review that you got if  
3 Westinghouse had submitted this and had done it in the  
4 first place?

5 The third round is that they don't do  
6 that. They leave the DAC. Now the DAC is there.  
7 What level of review, then, is done? How do the  
8 questioning, detail experts, and all that stuff, get  
9 done for that DAC resolution, once it is in place?

10 ME. JACKSON: Laura, do you want to --

11 MS. DUDES: Yes, I do.

12 Yes, I think you have gotten Option A,  
13 which is in the DCD, Option B, at the COL, Charlie,  
14 down. And then, I think your question, and we will  
15 get to it at the end of the presentation today because  
16 we have our plans for how we would approach this  
17 activity in an inspection realm. So we have an entire  
18 presentation that talks about that.

19 But, in short, what we are trying to  
20 demonstrate throughout the day is the regulatory  
21 activities associated with resources, expertise, and  
22 level and depth and scope of the activity to resolve  
23 DAC will remain the same across each one of the  
24 processes.

25 The hat that it wears, whether it is a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1     *licensing activity or an inspection activity, does*  
2     *change once the license is issued. However, the time,*  
3     *effort, expertise, and evaluation of the digital I&C*  
4     *system and the design will remain equivalent*  
5     *throughout all three processes.*

6             *CHAIRMAN BLEY: Okay, I don't want us to*  
7      *dwell on the process too much, but I did want to*  
8      *confirm that I understood things right.*

9             *At the COL stage, the COL applicant would*  
10     *in the same way submit an amendment to the DCD, is*  
11     *what was said.*

12            *MS. DUDES: No. Specifically --*

13            *CHAIRMAN BLEY: Say the process.*

14            *MS. DUDES: -- if you are going to resolve*  
15     *DAC at the COL -- you are referencing a certified*  
16     *design. You would actually just submit that*  
17     *information as part of your license application. It*  
18     *becomes part of your final safety analysis --*

19            *CHAIRMAN BLEY: You would identify that*  
20     *you are removing the DAC, I assume?*

21            *MS. DUDES: Yes, but you are not amending.*  
22     *You are not going backwards into the DCD. So that is*  
23     *actually just a site-specific license that resolves*  
24     *that DAC, and it is only applicable to that one*  
25     *license; whereas, an amendment is applicable to all.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Once we have amended the DCD, it can be referenced by  
2 numerous --

3 MEMBER ARMIJO: If that combined license  
4 is a referenced combined license, can another  
5 applicant, then, incorporate that by reference,  
6 including the resolved DAC?

7 MS. DUDES: They can incorporate the same  
8 information. You know, we are going to start to get  
9 into the legal distinction in terms of really the  
10 review. We would have to do the same review twice if  
11 it is a reference COL and a subsequent COL references  
12 the same information. It really becomes a matter of  
13 what issues are opening up for a mandatory period,  
14 what site-specific activities or licenses --

15 MEMBER ARMIJO: But as far as technical  
16 review, if it was really identical, it should be  
17 easy --

18 MS. DUDES: Yes, we could definitely take  
19 advantage of the resources that were spent on the  
20 reference COL.

21 MEMBER ARMIJO: Okay.

22 ME. JACKSON: So the final point I wanted  
23 to make on this slide here was that, in April of 2009,  
24 we conducted our first audit to verify that the DAC  
25 associated with the planning activities phase were

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 complete. That was a key part of being able to verify  
2 that Westinghouse actually had completed this software  
3 development phase.

4 So next slide.

5 So, in March of 2010, we conducted a  
6 second audit, and this was at Westinghouse's  
7 subsidiary, CS Innovations, which developed part of  
8 the PMS system. We primarily looked at the parts of  
9 the PMS that they were developing as well as they were  
10 developing the Diverse Actuation System.

11 In April of 2010, we did a third audit at  
12 Westinghouse's facilities to look at part of the  
13 planning phase, but also, in more large part, the  
14 requirement specification for the PMS and the verified  
15 completion of that.

16 **MEMBER BROWN:** You had those three audit  
17 reports, and if you go look at those audit reports,  
18 they are largely process audits. Correct me if I'm  
19 wrong. I mean you are looking at their specific  
20 process for their software development program, not at  
21 specific software that they were developing to  
22 implement or execute their design. That's the way,  
23 when I went through the audits quickly, that what it  
24 came out to me.

25 **ME. JACKSON:** I would say the ones for the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *planning phase, yes, we are looking at their software*  
2 *development process. So it was verifying the process*  
3 *itself was there and adequate, which is in large part*  
4 *what that first phase is for.*

5 *For the requirements specifications or*  
6 *system definition phase, Westinghouse identifies it,*  
7 *which is largely that that third audit, we actually*  
8 *looked at the requirements specifications themselves.*

9 *And if you look at that audit report, you will*  
10 *actually identify some examples where the staff didn't*  
11 *find certain requirements either clear or traceable*  
12 *within the requirements specification.*

13 *So we did not only just look at did they*  
14 *follow the process, but we actually looked at the*  
15 *output of that process, which was the requirements*  
16 *specifications, the requirements traceability, et*  
17 *cetera.*

18 *MEMBER BROWN: Yes, but the requirement*  
19 *specification/traceability is still largely a paper-*  
20 *process-type point.*

21 *ME. JACKSON: That's true. And actually,*  
22 *I'm kind of jumping ahead a little bit. But for the*  
23 *requirements specifications, for example, we took the*  
24 *DCD, which we look at and say this contains the high-*  
25 *level requirements, and we are looking at how they are*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 broken down into more detailed requirements.

2 So, we began there tracing, based on our  
3 knowledge of what we know about the system, and began  
4 asking questions about, is this requirement here? So  
5 part of that is the completeness aspect. Are all the  
6 requirements there that need to be there? And also,  
7 are they adequate?

8 So it was part process, but we did look at  
9 the product, too.

10 MEMBER BROWN: The product is really the  
11 code, and I don't mean source code. I mean the  
12 application code that actually executes and actually  
13 performs the function that the requirement --

14 ME. JACKSON: Yes, and at this time,  
15 Westinghouse was not at that --

16 MEMBER BROWN: Well, you don't have that  
17 yet. And that's one of the points of interest. For  
18 instance, if you are depending upon -- you know, all  
19 of these systems that you are working on right now are  
20 what I would refer to as highly-connected, you know,  
21 from train to train to train in terms of their  
22 software. In other words, they depend on software to  
23 ensure that the data and other information flow that  
24 goes between, from Division A and then to Division B,  
25 C, and D, is satisfactory.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           So, whether it is an authentication or an  
2           error-correcting code, or it is something else, the  
3           execution of that code, the results of that, that's  
4           what's important. The requirement is there that it  
5           work, but you don't know that it works until somebody  
6           tests and can demonstrate that all the possible  
7           combinations result in the correct combination coming  
8           out on the other end. And you can't do that. That's  
9           part of the design -- I put that in the design review  
10          category, not an inspection process category. So I am  
11          looking for how that part of this question gets  
12          involved.

13           ME. JACKSON: Okay.

14           MEMBER BROWN: I'll stop right there.

15           ME. JACKSON: So, basically, like if you  
16          look at the far lefthand column --

17           MEMBER BROWN: Am I clear, before you  
18          say --

19           ME. JACKSON: Yes, I understand what  
20          you're saying.

21           MEMBER BROWN: Thank you.

22           ME. JACKSON: And under 11(c),  
23          hardware/software development phase, this is largely I  
24          think what Charlie is talking about. This is where  
25          you are actually developing the code and you integrate

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that system.

2 And then, 11(d) is the system integration  
3 and test phase. This is actually where you are  
4 testing what you have developed, and you build a whole  
5 system, and you keep testing, and you are verifying  
6 the requirements as you are going. You are doing  
7 these tests, and so forth. Then the final phase is  
8 actually installing it in the plant itself.

9 So, at this time, those still remain as  
10 ITAAC, and they would be verified through the ITAAC  
11 verification process.

12 MEMBER BROWN: So the non-bolded stuff is  
13 ITAAC in your table?

14 ME. JACKSON: Correct.

15 Okay. So just the final point on this  
16 slide is that --

17 MEMBER BROWN: Before you go away -- I'm  
18 sorry -- if they eliminate 11, which 11 should have  
19 disappeared off the chart in their DAC --

20 ME. JACKSON: Not all of 11. Not all of  
21 11.

22 ME. SANTOS: You will see. We will show  
23 it.

24 ME. JACKSON: Yes, we will --

25 MEMBER BROWN: So the ITAAC part of this

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 would remain?

2 ME. ROGGENBRODT: Within the body of the  
3 example, we can clearly show that on the forthcoming  
4 slides --

5 MEMBER BROWN: All right.

6 ME. ROGGENBRODT: -- of how it went away,  
7 as you said.

8 MEMBER BROWN: And then came back? It was  
9 reincarnated.

10 ME. JACKSON: We will show you what  
11 Westinghouse proposed.

12 MEMBER BROWN: Okay. All right.

13 ME. JACKSON: We'll tell you what the  
14 results are.

15 MEMBER BROWN: Go ahead. Go ahead.

16 ME. JACKSON: So, from June to July, we  
17 had several other RAIs and interactions with  
18 Westinghouse, and we completed the staff's final  
19 Safety Evaluation Report, which was presented to the  
20 ACRS, and we had a meeting back in September.

21 So next slide.

22 These next four slides are going to show  
23 kind of the evolution from the certified design to  
24 what Westinghouse is currently proposing and what's on  
25 the docket. Now there is a Revision 18 that is

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 coming, and that will include commitments that  
2 Westinghouse has made to update the DCD, which  
3 includes the ITAAC, and so forth. We don't have that  
4 one on this slide.

5 There's two parts to Tier 1 information.  
6 So, for example, Tier 1, Chapter 2, Section 2.5.1,  
7 that just describes the Diverse Actuation System. And  
8 there's two parts. Part is called the design  
9 description, and the other part is the ITAAC itself.

10 And you can see in Revision 15, that's the  
11 certified design. So it had all the software  
12 development life cycle phases for DAS.

13 In Revision 16, they changed some wording.  
14 This was actually the amendment, the initial  
15 amendment, that was submitted.

16 And then, Revision 17, Westinghouse felt  
17 that they had completed the design requirements phase  
18 and system definition phase. So they removed that  
19 portion of the ITAAC in Revision 17. Now it's up to  
20 the staff to review and approve that, but that's where  
21 Westinghouse was when they submitted their  
22 application.

23 So, if we could go to the next slide?

24 And this is similar, except it is for the  
25 PMS. As you can see in this one, Revision 16

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 initially, they felt they were done with the design  
2 requirements or planning phase. Then, in Revision 17,  
3 they felt they were done also with the system  
4 definition phase. Now we will talk about the staff's  
5 conclusions toward the end of this slide presentation.

6 Okay, next slide there.

7 This is the ITAAC. So, similar to the  
8 design description, they were removing the particular  
9 software phases they felt they had completed.

10 And we can go to the next slide.

11 That was DAS and that's for PMS.

12 Okay. So now we begin to get into the  
13 actual example we wanted to discuss. I will first  
14 start off and talk about safety significance of,  
15 first, PMS, which it performs reactor trip, ESF  
16 actuations, and also provides qualified data  
17 processing functions. So it is a pretty important  
18 system in the AP1000.

19 Now the safety significance of the PMS  
20 design requirements or planning life cycle phase is  
21 that it identifies a high-quality process by which PMS  
22 hardware and software are design, fabricated,  
23 installed, and tested. This is a first step to ensure  
24 quality assurance.

25 Now, to get a high-quality PMS, there's

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 other steps in there. As Charlie had mentioned, you  
2 have to look at the design outputs as well. But this  
3 is a first step.

4 A good analogy for me is, if you think  
5 about welding, in welding you have procedures, and so  
6 forth, on how you do that. This is kind of like what  
7 that design requirements phase is, is those welding  
8 procedures.

9 Now you've got other steps where the guy  
10 welding actually has to be qualified, and he has to do  
11 the weld correctly, and then they have to test it.  
12 That is kind of synonymous to software development,  
13 where you go in, you do the actual design work, build  
14 it, and then you test it at the end to verify that it  
15 is an adequate system.

16 Okay. Next slide.

17 And what we are listing right here, these  
18 are the specific requirements that affect the AP1000  
19 PMS design requirements phase. These are four  
20 regulations, and I won't go through each one of them,  
21 but they basically require quality assurance.

22 The staff found that the AP1000 complied  
23 with these requirements in both the certified design  
24 as well as the amendment.

25 So, the next question is, well, what

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 acceptance criteria did the staff evaluate the  
2 applicant's submittals against?

3 MEMBER BROWN: Let me backtrack for just a  
4 second. I am going to use the welding analogy. Okay?

5 Because you say you define and you set up  
6 the welding process such that, theoretically, you get  
7 your desired results. Then you go actually do the  
8 weld. And then you go test it, okay, to see that you  
9 get it.

10 The thing you left out, when you related  
11 it to the PMS, in that first stage is when you develop  
12 a weld process, you actually define what your  
13 characteristics are. You say it will not have  
14 inclusions; it will not have this; it will not have  
15 that. So those items are all listed and identified as  
16 fundamentally acceptance criteria for the development  
17 of that weld process.

18 And all you do, then, in the testing  
19 phase, again -- and all their qualification, all the  
20 work that goes into qualifying that welding process is  
21 based on it, and you have those listed upfront.

22 ME. JACKSON: Right.

23 MEMBER BROWN: If I go to the PMS thing,  
24 it says, hey, you're going to have a hardware and  
25 software development and implementation, and then a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 system integration and then an installation. Whatever  
2 it is, you've got three different things left over.

3 If you go look in the DCD or you go look  
4 in the ITAAC or you look in the DAC, some of the stuff  
5 that was missing were the specifics. In other words,  
6 what is the authentication code or what is it supposed  
7 to detect?

8 ME. JACKSON: Right.

9 MEMBER BROWN: How is it? So that's  
10 missing. That is one of the items that is missing  
11 when we go through a design certification. At least I  
12 didn't find it. So that is one of the concerns, and I  
13 just wanted to bring up the analogy as not quite  
14 apples and apples.

15 ME. JACKSON: Right. Well, I do want to,  
16 and I hope we address that in your presentation. If  
17 we don't, let us know.

18 MEMBER BROWN: I'm just letting you know  
19 what I'm looking for. That's all.

20 ME. JACKSON: And basically, like on this  
21 slide here that Dan has, I think we are actually  
22 starting to get into it because, if you look at, say,  
23 the PMS, DAC, ITAAC that we showed earlier, yes, if  
24 you look at it just alone, it looks pretty skimpy.  
25 But the staff uses the licensing basis, which is

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 contained in the DCD, to also say this is how they met  
2 that ITAAC.

3 And there's a lot of information that is  
4 back behind that inside a DCD. So, for example, like  
5 we'll start off with this slide here. Westinghouse,  
6 as a first step, they committed to follow the guidance  
7 in Regulatory Guides. And again, this is the process  
8 for a software and life cycle development process.  
9 And this is in Chapter 1, Tier 2, Appendix 1A. So  
10 they say it conforms to all these. Now that provides  
11 a lot of criteria with regard to how you do the  
12 software development process.

13 But to get to your point with regards to  
14 characteristics of the PMS itself, there's other  
15 technical reports, and so forth, which also define  
16 that. So, for example, they range from the Common Q  
17 topical report -- in the software program manual,  
18 there was two technical reports. One was on PMS  
19 architecture itself, as well as there was one on data  
20 communication or two on data communications, I think.

21 So there's numerous documents which are  
22 behind this here that contain a lot of criteria. So  
23 it is not just that ITAAC itself, but the staff uses  
24 this to verify that the DAC ITAAC is actually complete  
25 using the licensing basis.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   ME. ROGGENBRODT:     Going back to our  
2     example, in the planning activities phase, we have  
3     some note we could potentially go to in the  
4     requirements phase after the presentation, if it is  
5     deemed necessary.

6                   ME. JACKSON:   Continue? Okay.

7                   So, in addition to the Regulatory Guides,  
8     Westinghouse also had their commitment with regards to  
9     HICB-14. Now that was the predecessor to BTP-714 and  
10    the Standard Review Plan, and that is guidance on  
11    software reviews for digital computer-based I&C  
12    systems. That commitment is located in Tier 2,  
13    Section 1.9.2, and that is via WCAP-15799.

14                  Then, in addition to that, Westinghouse  
15    has two reports. One is the Software Program Manual  
16    for the Common Q system. That was identified as Tier  
17    2\*. What that means, then, the DCD, is that the  
18    vendor and the licensee cannot change that document  
19    without prior NRC approval or change it and use it in  
20    the development of the software without prior NRC  
21    approval.

22                  There's also a companion document with  
23    that. That is WCAP-15927. That relates specifically  
24    to a design process for AP1000 Common Q safety  
25    systems. That is Tier 2\* as well.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   *Next slide.*

2                   *So this just shows, this is a slide that*  
3 *actually comes out of HICB 7-14. This is just*  
4 *identifying the different components of the planning*  
5 *activities phase. So, for example, you can see in the*  
6 *far lefthand corner there is Software Management Plan*  
7 *all the way down through Software Configuration*  
8 *Management Plan.*

9                   *And when the staff did our audits at*  
10 *Westinghouse, we looked at these specific plans, which*  
11 *were encapsulated by Westinghouse procedures at their*  
12 *facility.*

13                   *And these plans as well, they are also*  
14 *described with the Common Q software program manual*  
15 *and the WCAP-15927 document.*

16                   *So this is just to talk about the*  
17 *certified design. In 2006, in Section 7.1.4 of*  
18 *NUREG-1793, which was the staff's FSER --*

19                   *CHAIRMAN BLEY: Can you back up to that*  
20 *last slide?*

21                   *ME. JACKSON: Uh-hum.*

22                   *CHAIRMAN BLEY: When you go to visit and*  
23 *do an audit, and I'm not sure which of these things*  
24 *were done at the time you were there, but let's just*  
25 *pick one. Design Activities, and you get down at the*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 bottom, Design Safety Analysis, and the V&V Design  
2 Analysis. These are things in your audit you would  
3 look through and ensure that they are doing these in  
4 the way -- it looks like at that point it's not just  
5 process; it's actual safety analysis.

6 ME. JACKSON: Right. In fact, maybe a  
7 good example is the one beside it, the Requirements  
8 Activities phase. That one also has a Requirements  
9 Safety Analysis, a V&V Requirement Analysis Report,  
10 and a Configuration Management Requirements Report.

11 So, when we did the audit, we looked at  
12 those analyses as well as the requirements  
13 specifications themselves.

14 CHAIRMAN BLEY: Now those could have led  
15 to RAIs or did, or you were able to resolve things  
16 while you were there?

17 ME. JACKSON: As we get into the example,  
18 you will see where in some cases we identified some  
19 issues.

20 CHAIRMAN BLEY: Okay. So the example will  
21 look at this kind of thing?

22 ME. JACKSON: Right. Now, for example,  
23 like in the Requirements Activities phase, I mean if  
24 we go in and we find maybe one or two minor issues out  
25 of, say, a sample of 60 requirements and stuff, we

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 would probably look at that and say, well, okay, you  
2 should put that in your corrective action program,  
3 because Westinghouse has an Appendix B program. So,  
4 they should put that in there and they should resolve  
5 it.

6 And we would note it in our audit report,  
7 so that future audits or inspections, they could come  
8 back and verify that Westinghouse is actually  
9 following through on their corrective actions.

10 Now, if we go in and we find a number of  
11 issues or we find kind of a similar theme of issues,  
12 then that gives the staff pause, and we have to step  
13 back and look and say, well, should we approve, in  
14 this case, like the removal of the requirements  
15 activities at this time? And if there is a high  
16 number of issues or there is a common theme through  
17 there, then we have to really think about that.

18 And in this process, which is the  
19 amendment process, ultimately, Westinghouse is seeking  
20 approval to remove the ITAAC or that part of the DAC.

21 In the case, kind of jumping ahead, what you will see  
22 is we didn't approve the removal of the system  
23 definition phase from the ITAAC. So that will be  
24 coming back into Revision 18.

25 CHAIRMAN BLEY: And just this example

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 might not fit, but some other one would be parallel.  
2 If it is done post-COL, you would still go audit the  
3 detailed reports and raise issues. But to get closure  
4 on them, either it would have to be an agreement on  
5 the spot or you would have to issue findings or --

6 ME. SANTOS: It will be on inspection, and  
7 we will cover that through the other -- this is Dan  
8 Santos from the staff. We will cover that through the  
9 ESBWR example, where in the inspection phase what are  
10 the expectations and the process.

11 MEMBER BROWN: We are on AP1000 now.

12 ME. SANTOS: Well, the answer was --

13 CHAIRMAN BLEY: That's okay.

14 MEMBER BROWN: I know, but I mean I don't  
15 want to mix --

16 CHAIRMAN BLEY: No, he's not. He's going  
17 to do it later.

18 MEMBER BROWN: Yes, but your question is,  
19 when they look at the Requirements Safety Analysis,  
20 for instance, it is a matter of, what are you looking  
21 at? Let me stick with this right now.

22 CHAIRMAN BLEY: Yes.

23 MEMBER BROWN: What are you looking at  
24 when you look at that? I mean you haven't written the  
25 software yet. All you have done is said you have told

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 people that you want the requirements incorporated  
2 into the program code, the application code. So that  
3 is still a process-type issue, but all it is verifying  
4 is that we took stuff from up here and it is in the  
5 instructions to go do that.

6 ME. SANTOS: They have more than that.  
7 Not only do they have the high level, but they have  
8 like detailed -- they are now starting to populate  
9 with the detailed --

10 MEMBER BROWN: Populate what?

11 ME. SANTOS: Their requirements --

12 MEMBER BROWN: Of a phase, a process  
13 phase, in other words?

14 ME. JACKSON: Let me maybe, and then I  
15 will pass it off to Bill here because he was there on  
16 the team as well.

17 For requirements specifications, as a  
18 minimum, we expected the requirements of the DCD to  
19 also be in their requirements specifications that they  
20 are going to use to build a system. So that was a  
21 first start.

22 Now those are more high-level, and  
23 eventually you have to break them down into software  
24 requirements specifications or hardware requirements  
25 specifications. And we expect to see that as well.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           And there will be other requirements in  
2 there or maybe for the form or features of the PMS  
3 which really don't have any kind of regulatory  
4 bearance, and those they can add in there as well, to  
5 be able to track those requirements.

6           But I will pass it off to Bill to comment.

7           ME. ROGGENBRODT: Good afternoon. This is  
8 Bill Roggenbrodt from the Division of Engineering  
9 Branch 1.

10           Just to follow along with this, I believe  
11 if you will allow us to get through this one example,  
12 we can answer many of those questions. Again, in a  
13 planning activities phase, I could discuss, actually,  
14 Charlie, to your point, some of the product issues,  
15 like how are you going to ensure this or what was the  
16 demonstration that helped you verify that they are  
17 following the process for a completed product. I  
18 could do that, but I don't think I could do that in  
19 the open portion of this meeting.

20           MEMBER BROWN: Okay, go on.

21           ME. SANTOS: Very quick, Charlie, what you  
22 are asking for is implementation integration  
23 activities.

24           MEMBER BROWN: Yes.

25           ME. SANTOS: So that's later in the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 process and this will be ITAACs, which will be done  
2 through an inspection activity, and we will cover how  
3 that is going to actually get done.

4 But your code and the real beef is  
5 following --

6 MEMBER BROWN: Some stuff can be done this  
7 way, and some I have difficulties with.

8 ME. SANTOS: Okay.

9 MEMBER BROWN: Okay. So go ahead.

10 ME. JACKSON: All right. So, on the next  
11 slide there, Dan, I was talking about the staff's  
12 original approval for the current certified design,  
13 and the staff accepts the use of DAC for the certified  
14 design, since PMS was characterized as rapidly-  
15 changing technology. Really not the system, but,  
16 well, it's the technology, the platforms in there were  
17 characterized as rapidly-changing technology, as  
18 discussed in SECY-02-0059, and this is where the  
19 Commission accepted the use of DAC in the certified  
20 design.

21 The design commitments in AP1000, Tier 1  
22 and Tier 2, as well as the DAC/ITAC, provide those  
23 procedures and attributes necessary for the staff to  
24 reach a reasonable assurance of the safety finding.

25 And I would just comment on maybe the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *changing technology. There were some changes, as*  
2 *Westinghouse went from Revision 15 to Revision 17. In*  
3 *some cases, it was for particular safety improvements.*

4 *For example, they had multiplexers in the*  
5 *original design. The amendment removed those. That*  
6 *was actually a safety improvement because the*  
7 *multiplexers, if they failed, they affect multiple*  
8 *functions; whereas, with the current design, it is*  
9 *more distributed, and so, therefore, a single failure*  
10 *has less effect on other functions.*

11 *MEMBER BROWN: Fine, but that is not*  
12 *evolving technology. Multiplexers have been around*  
13 *and the stuff that replaced them has been around for*  
14 *decades.*

15 *ME. JACKSON: Well, yes, I mean there's --*

16 *MEMBER BROWN: It is just a matter of a*  
17 *design choice. It's a better design to not use*  
18 *multiplexers than it is to use discrete functions to*  
19 *transmit your data from point parameters up into the*  
20 *mainframe; that's all. It's a design decision. It*  
21 *has nothing to do with evolving technologies. That's*  
22 *the only point.*

23 *ME. ROGGENBRODT: This is Bill Roggenbrodt*  
24 *again.*

25 *I agree with your point. I think the*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 point that Mr. Jackson was trying to make was that it  
2 was sort of a generic safety improvement or  
3 enhancement, a multiplexer --

4 MEMBER BROWN: Well, I won't disagree with  
5 that. I'm not disagreeing with that.

6 ME. ROGGENBRODT: So, not getting down to  
7 specifics, I would agree that it wasn't that.

8 MEMBER BROWN: Okay.

9 ME. JACKSON: So, on the next slide, for  
10 the proposed AP1000 amendment, and this is in addition  
11 to the DCD itself, Westinghouse submitted 29 documents  
12 related to the PMS and planning and requirements  
13 phase.

14 As, Charlie, you had mentioned when you  
15 were talking about characteristics, and so forth,  
16 these are some of the documents that contain those  
17 characteristics which the PMS should have when it is  
18 finally designed and constructed.

19 And the staff -- and part of these  
20 documents were part of those 29 documents, and this is  
21 where the staff reviewed these. So we evaluated each  
22 one of them one-by-one.

23 Now, on the next slide, staff evaluated,  
24 in addition to reviewing those 29 documents, we  
25 evaluated over 100 Westinghouse proprietary documents

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 related to the design requirements and system  
2 definition phases of DAS and PMS development.

3 And when we say that it is Westinghouse  
4 proprietary documents, these are engineering  
5 procedures and documents that they have at their  
6 facilities that they use to actually build the systems  
7 with. So these were all done through audits, and  
8 there were three of them.

9 Then, the review and audit teams that we  
10 used, they consisted of staff members from I&C, from  
11 Human Factors Engineering, Technical Specifications  
12 Branch, the Plant Systems Branch; as well, we had two  
13 Region II construction inspection staff that were part  
14 of our audit team as we were going through these  
15 audits.

16 So, overall, in the three-and-a-half years  
17 since NRO began reviewing the AP1000 amendment, we  
18 have spent over 5,000 man-hours on the AP1000 DCA  
19 review. Now that is not just the DAC removal, but  
20 that is for everything. And there were 113 Requests  
21 for Additional Information. Again, that is not just  
22 related to the DAC, but that is in total for the I&C.  
23 And we reviewed over 6,000 pages of docketed  
24 information.

25 So, to talk a little bit about some of the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 issues that we identified when we were going through  
2 the DAC review process, in particular, the staff sent  
3 a letter to Westinghouse in March of 2009 regarding  
4 technical issues identified during the document  
5 reviews as well as in the audits. Westinghouse  
6 replied to us in April of 2009.

7 And as you can see, there were six issues  
8 there that ranged from the Component Interface Module,  
9 which is part of the PMS; Diversity and Defense-in-  
10 Depth Analysis; the DAS development documents; the  
11 testing methodology; revised technical reports, and  
12 the computer security plan.

13 You noticed that all but one of them is  
14 highlighted. And the reason that they are highlighted  
15 is because those issues did impact part of the DAC  
16 removal. So there are other aspects, and they tied in  
17 with the DAC removal here.

18 Okay. So Laura has shown this slide  
19 earlier. This is where we are going to really narrow  
20 down into a particular example.

21 In the I&C review, there's various copies  
22 that we review. That includes like the design basis  
23 functions of I&C, which is reactor trip, ESF  
24 functions, as well as safe shutdown, information  
25 displays --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1                    *MEMBER BROWN: Could I ask you to hold on*  
2 *for a minute?*

3                    *My handout goes from slide 31 to 43.*  
4 *Could we get another one?*

5                    *MS. DUDES: Charlie, you can have mine.*

6                    *MEMBER BROWN: Oh, there we go.*

7                    *MS. DUDES: No problem.*

8                    *(Laughter.)*

9                    *MEMBER BROWN: I thought that one was a*  
10 *little thin.*

11                   *CHAIRMAN BLEY: It had your name on it, I*  
12 *think, Charlie.*

13                   *(Laughter.)*

14                   *ME. JACKSON: Okay. So we have looked at*  
15 *various topics, control systems, defense-in-depth. So*  
16 *what we are doing is our example is going to focus in*  
17 *on the PMS life cycle, which was part of Section 7.1*  
18 *of the DCD.*

19                   *Next slide.*

20                   *Within the PMS life cycle, you've got*  
21 *various phases which we talked about earlier. The one*  
22 *we are going to narrow in on is the planning*  
23 *activities.*

24                   *So, next slide.*

25                   *So, with that, we are even going to narrow*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 it down even further because, within the planning  
2 activities phase, remember, we showed the list of all  
3 the different types of plans between Software  
4 Management Plan all the way down to Software  
5 Configuration Management.

6 As I mentioned, we are going to focus in  
7 on the Software Verification and Validation Plan. I  
8 know it is a process, but it is one of the key  
9 processes that the staff uses to ensure adequate  
10 safety because that is the part where it gets  
11 independent review by the vendor or the licensee to  
12 verify that the system can perform its function as  
13 expected.

14 What we hope to do with this example is to  
15 show the level of depth to which the staff reviewed  
16 the detailed design material. This did involve  
17 issuing an RAI and, as well, doing audits. But,  
18 again, this was in the review process, so we had the  
19 tool of an RAI, but in other aspects we didn't use  
20 RAIs. It was just an audit where we went out to  
21 confirm something.

22 The staff used several tools during our  
23 review. And primarily, we used HICB-14, in  
24 particular, Section B.3.1.10, as well as Regulatory  
25 Guide 1.168, which endorses two IEEE standards, 1012

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and 1028.

2 And there was another tool that we used  
3 that is not specifically endorsed or called out, but  
4 it is NUREG CR-6101. That was a helpful document. It  
5 gets in a little more depth. You will find in our  
6 later slides that that document was also used to  
7 develop the DAC inspection procedures as well.

8 So, during the review of the AP1000, we  
9 discovered a problem with regard to independent V&V.  
10 If you remember, we talked about Tier 2 documents.  
11 One of them was WCAP-15927. Bill, during his review,  
12 he noticed that it was removed. So he wanted to find  
13 out, well, what was the importance of that document.

14 What he found out was that in the original  
15 review, in response to an RAI, Westinghouse provided  
16 additional measures for the Common Q software  
17 development process, in addition to what was in the  
18 SPM. So, this WCAP-15927 discussed how the  
19 application-specific Common Q software life cycle  
20 development process would conduct independent V&V  
21 activities, in particular.

22 So, due to the additional commitments in  
23 the WCAP, the independent V&V activities would be  
24 handled exclusively by the independent V&V  
25 organization, which is normally what you would expect.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1       *That would satisfy particular regulation, which is*  
2 *Appendix B, Criterion 3.*

3               *Under the Common Q SPM, either the design*  
4 *team or the V&V team could be responsible for testing*  
5 *during the phases of Common Q development. So we saw*  
6 *that as problematic.*

7               *Next slide.*

8               *So, when Westinghouse removed -- well,*  
9 *actually, the staff originally, when we got the*  
10 *revision to the DCD, we saw this Tier 2 document was*  
11 *removed, and Bill noted that, well, there was a change*  
12 *in the independent V&V aspect. So he initially issued*  
13 *an RAI with regards to that.*

14               *So, basically, he issued the RAI, and then*  
15 *Dan, on the next slide, this just shows there were two*  
16 *documents, actually, two Tier 2\* documents*  
17 *Westinghouse removed. One of them was the one we are*  
18 *talking about, and the other had to do with a Visual*  
19 *platform called Eagle 21. In the original*  
20 *certification, the AP1000 could use either platform,*  
21 *but Westinghouse decided to remove the Eagle 21 out*  
22 *completely. So, this document described the Eagle 21*  
23 *system. So, we felt, yes, it is appropriate to remove*  
24 *it out if you are not going to use the platform.*

25               *Next slide.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           So Westinghouse responded to our RAI, and  
2 they noted that the SPM is a Tier 2 document. It  
3 addresses the items requested in the original RAI.  
4 They noted that the NRC stated in its SER for a Common  
5 Q platform that the Common Q SPM specifies plans for  
6 implementing a structured software life cycle process  
7 for application software and provide guidance for  
8 configuration management of commercial grade hardware  
9 and previously developed software.

10           So, they felt that the issue regarding  
11 modular testing was subsequently closed in the NRC's  
12 SER for the Common Q SPM, and therefore, the original  
13 request for docketed design process information was  
14 fulfilled by the SPM for Common Q systems.

15           So, going on to the next slide there, Dan,  
16 now the staff, we observed that the response didn't  
17 adequately address the questions that we posed.  
18 Particularly, we reviewed the Common Q SPM, and  
19 there's a particular exhibit in there, Exhibit 5.1,  
20 that allowed either the design team or the  
21 verification team to perform testing on the equipment  
22 that is developed by the design team for the  
23 protection system. We didn't feel that this was  
24 appropriate to meet, in particular, Appendix B,  
25 Criterion 3. So Revision 0 of WCAP-15927 provided the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 *measure to provide that independent V&V. Therefore,*  
2 *it was necessary.*

3 *So, then, the next step was the staff went*  
4 *and did an audit at Westinghouse's facility, and we*  
5 *looked at the actual V&V procedure that Westinghouse*  
6 *uses for conducting their activities. And what we*  
7 *noted during our audit was that this document stated a*  
8 *commitment to follow IEEE 1012. However, we noted*  
9 *that the document was a V&V process for generic Common*  
10 *Q equipment and not application-specific equipment,*  
11 *such as AP1000.*

12 *And IEEE 1012 requires requirement*  
13 *traceability analysis to be conducted by the V&V team,*  
14 *as does the Revision 0 WCAP-15927. So Bill noted that*  
15 *the current document Revision 3 had been issued in*  
16 *August 2008, and upon presentation with the revision*  
17 *of the document in effect during certification, the*  
18 *text also committed to follow IEEE 1012 implicitly*  
19 *without regard to the SPM.*

20 *So Westinghouse responded by providing a*  
21 *draft Revision 1 to WCAP-15927 during the audit. So*  
22 *they showed us this is a draft of how we can change*  
23 *the process.*

24 *The document allowed the design team to*  
25 *conduct the requirement traceability rather than the*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 independent V&V team. So we informed them that the  
2 document in its current form would not be accepted as  
3 a replacement for Revision 0. So Westinghouse  
4 modified their software independent V&V procedure,  
5 such that now the functions of developing a  
6 requirements traceability matrix and the requirements  
7 for traceability analysis will be split out between  
8 the design team and the V&V team.

9 So the issue that Westinghouse had was  
10 that the design team generates the requirements. That  
11 is part of their activities. So they wanted to be  
12 able to explain that the design team, they will  
13 generate these requirements, and they have to put it  
14 into the requirements traceability matrix.

15 But our issue was, well, the analysis has  
16 to be done by the independent V&V team. So what they  
17 changed to was actually to have the independent V&V  
18 team will now do the requirements traceability  
19 analysis once the design team has populated the  
20 requirements traceability matrix. So we found that  
21 that was an acceptable design there.

22 And, Dan, if you will go to the next  
23 slide --

24 **MEMBER BROWN:** At the end of this, it says  
25 that they redocketed 15927, Rev 2. What's --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   ME. JACKSON:    Okay.    On the next slide  
2 there it will show Revision 2 to change it --

3                   ME. ROGGENBRODT:  This is Bill Roggenbrodt  
4 again.

5                   The top of the previous slide speaks to  
6 Revision 1 of the document, and Revision 2 is the one  
7 that had the necessary change and the necessary  
8 splitout, if you will, of the design team performing  
9 the requirements traceability matrix for generating  
10 the requirements and tracking them, and the  
11 requirements traceability analysis being allied to the  
12 verification team exclusively.

13                  MEMBER BROWN:  So was 15927 put back into  
14 the Rev 17?

15                  ME. ROGGENBRODT:  That is a Westinghouse  
16 commitment for --

17                  MEMBER BROWN:  For 18?

18                  ME. ROGGENBRODT:  Correct.

19                  MEMBER BROWN:  Okay.  So it is splitting  
20 out the design and verification activities --

21                  ME. ROGGENBRODT:  Correct.

22                  MEMBER BROWN:  -- as opposed to being done  
23 by allowing it to be done by one guy?

24                  ME.    ROGGENBRODT:        Correct.        That's  
25 correct.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           MEMBER BROWN: It is now back in the DCD?

2           ME. ROGGENBRODT: Correct.

3           ME. JACKSON: So our purpose there in  
4 describing this whole example was to show you that  
5 this was one specific issue within the entire design  
6 which we really traced down in using our audits, and  
7 so forth. So, when we do the audits, which, you know,  
8 we hope to show that -- well, the activities we do in  
9 the audits is very similar to what we do in  
10 inspection, and we are able to ask questions that we  
11 need to ask and to look at documents we need to look  
12 at, and eventually, come to a resolution on specific  
13 technical issues such as this one.

14           This concludes this particular example,  
15 where we felt that it was a success in the efforts the  
16 staff used to be able to conclude as part -- now  
17 there's other parts of it, but in part of the  
18 conclusion that the Design Acceptance Criteria was  
19 able to be closed out.

20           Okay, the next slide there, Dan.

21           So this is a little bit about the PMS DAC  
22 review conclusion that the staff came to. So, based  
23 on both the review we did and the audits we conducted,  
24 we found that the design requirements or the planning  
25 activities phase of the PMS development process was

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 considered complete with one exception, and that had  
2 to do with the CIM life cycle development process  
3 would remain as DAC in Tier 1 of the AP1000 DCD.

4 The reason for that is because we felt the  
5 process that was described in the engineering  
6 documents we saw was still insufficient for the staff  
7 to conclude it met regulations or satisfied associated  
8 guidance which was in the DCD already.

9 So that is another example of where we  
10 went out and we, through our audits, we were  
11 verifying, are they meeting the commitments in the  
12 DCD? And what we found was, no, in this case. So the  
13 staff's response was, well, this still needs to be,  
14 still remain within the DCD itself, this ITAAC.

15 In fact, the next slide will show it is a  
16 new ITAAC. They actually removed the design  
17 requirements phase out of the PMS, and they developed  
18 a new ITAAC, which is considered DAC. This is just  
19 for the component interface model.

20 If you could go back to the previous slide  
21 there, Dan, another conclusion that we had, if you  
22 remember, for the PMS DAC, Westinghouse felt that they  
23 had completed the system definition phase, which was  
24 requirement specification activities. And we did not  
25 feel that was completed, either. That was based on

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the results of three audits that we conducted. And  
2 basically, the issues that we saw was either one of  
3 completeness of the requirements or there was an issue  
4 with traceability. Those were the two primary issues  
5 that we identified.

6 But, in order to do that, we had to get  
7 into the requirements specifications themselves. So,  
8 in that audit that we did, we selected -- and we had a  
9 team of about eight people -- we selected about 60  
10 requirements and went through them. And each one  
11 takes some time to go through because, as we drill  
12 down into them, you know, there's some discussion,  
13 interviews with Westinghouse staff, you know, trying  
14 to clarify and understand what exactly they were  
15 doing.

16 So, based on that audit, which was a week-  
17 long audit -- it probably took about a month's time  
18 overall from planning to actual documentation of the  
19 audit report -- we were able to arrive at a conclusion  
20 for that particular life cycle phase.

21 ME. SANTOS: That's not just an audit.  
22 They would read all the documents --

23 ME. JACKSON: Right. Well, we used the  
24 documents here. For example, as I said before, in our  
25 audit we would take the information that was docketed

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and say, okay, as a starting point, these should  
2 contain requirements that you should at least have in  
3 there. So we would pick samples of different ones,  
4 and then we would drive down in detail and say, well,  
5 okay, for one, how can I trace between where did this  
6 original requirement come from? And then, two, we  
7 would look at it and say, well, is it necessarily  
8 complete? Does it provide sufficient information  
9 whereby a software developer later on can actually use  
10 this, and when you are using it to test, will it give  
11 you a complete test?

12 All right. So --

13 CHAIRMAN BLEY: Charlie, go ahead.

14 MEMBER BROWN: Yes. Back on slide 27, you  
15 started there, or roughly started there, for this  
16 basic walkthrough of everything that you just did.  
17 And it says safety system life cycle development  
18 process. You didn't use the word "software", but  
19 that's all you talked about in the next 17 or 18  
20 pages. Okay? And that's one column, one stovepipe on  
21 here.

22 This is where -- and correct me if I'm  
23 wrong, because I'm trying to gain an understanding  
24 here -- how many of these columns do you complete in  
25 your certification process?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           ME. JACKSON: For the AP1000 amendment --

2           MEMBER BROWN: Column 1?

3           ME. JACKSON: -- we did review and audit  
4 activities in the first and second column.

5           MEMBER BROWN: The first and second  
6 columns?

7           ME. JACKSON: Right. The other ones are  
8 ITAAC that will be completed at a later date.

9           ME. SANTOS: Correct.

10          MEMBER BROWN: Okay. Do you have an  
11 example as opposed to the software, which is a review  
12 that is fairly aimed -- no, I guess it's set up, it's  
13 got to be a process-type review, just based on that's  
14 what it is. I mean a software programming application  
15 gets done so far down the line.

16                 So I guess my question is, when you do the  
17 design activities and you look at design  
18 specifications, hardware/software architecture, that  
19 has probably been where, at least from my viewpoint, a  
20 large number of my questions have originated.

21          ME. SANTOS: Correct. We are not there  
22 yet.

23          MEMBER BROWN: So you are going to do  
24 that?

25          ME. SANTOS: Correct. The expectation is,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 once that eventually they decide to close the --

2 *MEMBER BROWN: On the AP1000?*

3 *ME. SANTOS: On the AP1000.*

4 *MEMBER BROWN: No, no. When are you going*  
5 *to do that?*

6 *ME. JACKSON: Well, I would say, Charlie,*  
7 *as I was maybe trying to point out earlier, when we*  
8 *did our audit on the requirements activities, for*  
9 *example, one area, one of my staff members took the*  
10 *area of data communications and said, okay, pick some*  
11 *samples out of data communications and verify*  
12 *independence, et cetera, for that. So she went and*  
13 *did that and looked at several of those. So that is*  
14 *where, even though we are involved with the process*  
15 *there, we are beginning to look at the actual product.*

16 *Especially for safety-related or high-*  
17 *reliability systems, if there is going to be an error*  
18 *in the system, it is probably going to originate from*  
19 *the requirements being inadequate in some degree.*  
20 *That is what a lot of the experts have said.*

21 *So we wanted to focus a lot of attention*  
22 *on requirements specifications to make sure that --*

23 *ME. SANTOS: But to your question, it is*  
24 *better, then, to find out a time today to have the*  
25 *applicant probably answer that, because they are the*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *ones responsible for closing the ITAAC. So, when they*  
2 *explain their schedules for closing those ITAACs --*

3 *MEMBER BROWN: Okay. Stop right there.*  
4 *Okay?*

5 *ME. SANTOS: Okay.*

6 *MEMBER BROWN: I understand that, that*  
7 *that's the way it is going. The point is that you've*  
8 *got to have acceptance criteria for closing even the*  
9 *ITAAC that represent the actual things you expect to*  
10 *be validated.*

11 *ME. SANTOS: That's over there.*

12 *MEMBER BROWN: Well, we could talk about*  
13 *that for the next week and a half.*

14 *CHAIRMAN BLEY: We can talk some now. We*  
15 *have a little time. We are ahead a bit.*

16 *MEMBER BROWN: Yes. I don't want to*  
17 *get --*

18 *ME. SANTOS: But we should because that is*  
19 *where it resides. It resides in the DCD.*

20 *MEMBER BROWN: Let me pick one realm*  
21 *you're talking. You talk about the Common Q platform,*  
22 *and you lifted all the pieces of paper and everything*  
23 *else.*

24 *One of the elements for deterministic*  
25 *behavior is just a flat statement: it's deterministic*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 as long as the loading of the software, the  
2 application code and everything in it, is less than 70  
3 percent of the whatever sum, sample times, overall  
4 processing time, whatever that thing is, because it is  
5 an interrupt-driven system.

6 But there is no statement anywhere, or I  
7 didn't find anything, in the Common Q platform topical  
8 report that went in and developed an analytical basis  
9 for why 70 percent was a valid value. I mean, why  
10 does that make it okay? Is 80 percent okay? Is 50  
11 percent? If you are down to 1 percent, does it  
12 operate faster? Why is 70 percent picked?

13 And if you are going to go implement that,  
14 then you go look at your ITAAC to see, how do you test  
15 from plant parameter input to control device actuation  
16 via time response testing, which you have in there,  
17 how do you test that with a 70 percent load in the  
18 application code and its overall processing space?  
19 That's not called out anywhere.

20 And probably based on the modules that  
21 they have got in there, they are probably not loaded  
22 to 70 percent, at least in the initial setup, I'm  
23 guessing. That is a speculation on my part. But  
24 there is a key piece of the Common Q platform that is  
25 a specific technical statement that they make with a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *specific set of loading in their overall processing*  
2 *space. And yet, there is no addressing of that in*  
3 *terms of how do you validate or test for that when you*  
4 *finally design the system. I'm not saying you have to*  
5 *do it before, but that should be in there.*

6 *So that is not an acceptance criteria that*  
7 *says that, when you perform your final testing, time*  
8 *response testing, you actually have to load the thing*  
9 *up because people may make changes. They may add*  
10 *functions; they may add modules or products to it that*  
11 *they want to accomplish later, whatever the process is*  
12 *for that. And so, how do you make sure within the*  
13 *design space you have certified that it will actually*  
14 *perform as required?*

15 *I mean that is an example in the software*  
16 *area of putting a specific thing that you know is*  
17 *critical to the performance of the process --*

18 *ME. JACKSON: I can maybe address that in*  
19 *two parts. I think this issue was brought up at an*  
20 *earlier meeting, and we actually plan to address that*  
21 *in the November 2nd meeting, Subcommittee meeting,*  
22 *with the ACRS --*

23 *MEMBER BROWN: Okay.*

24 *ME. JACKSON: -- with regards to that*  
25 *specific aspect.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           But with regards to the DAC and the  
2           criteria, and so forth, for example, when we looked at  
3           the requirements specifications for AP1000, we would  
4           expect that they have that 70 percent loading criteria  
5           as part of the requirements specification. Now that  
6           starts out at a high level.

7           Now, as the design gets more involved,  
8           they have got to break it down and they have got to  
9           say we've got a certain process that runs this long, a  
10          certain process that runs this long, a certain process  
11          that runs this long.

12          And they have to do, just for example,  
13          like you have got design safety analysis here. They  
14          have to do that analysis to show that, yes, this is  
15          going to be okay as a design.

16                 ME. SANTOS: All the way to Chapter 15.

17                 ME. JACKSON: Right.

18                 MEMBER BROWN: I understand that part.  
19          The analysis is fine, but sometimes analysis is  
20          analysis, but test is test.

21                 ME. JACKSON: Right. And then, what I was  
22          going to finish saying is that, once it is identified  
23          as a requirement specification, and it goes down from  
24          high level to low level, when you go back up and you  
25          are doing your unit testing, your integration testing,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and finally your factory acceptance testing, they have  
2 to match up with all those requirements going back  
3 across. That is the expectation the staff has, and  
4 that is actually what they committed to in their DCD  
5 to do.

6 So there is testing at the detailed level  
7 with detailed criteria first, and as they go up and  
8 the system gets integrated and built, then they test  
9 at the higher levels to ensure that --

10 MEMBER BROWN: I read the entire chapter  
11 and I didn't see that explicitly. I read the topical  
12 report and I didn't see it. And I read 16675 and I  
13 didn't see it. Now it might be in there. It is just  
14 that that's a lot of pages.

15 ME. ROGGENBRODT: This is Bill Roggenbrodt  
16 from Branch 1.

17 To that end, I can support your finding  
18 that there was no detailed information to that level  
19 in dealing with this process for the past three years,  
20 nor would I expect it at this stage of the game, if  
21 you will.

22 The reason being is what you are getting  
23 down to is how the procedure, the testing procedure  
24 itself, is going --

25 MEMBER BROWN: No. No, I'm not asking for

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that. No. There is a specific set of criteria in the  
2 topical report. It says for satisfactory operation it  
3 has got to be loaded no more than "X".

4 ME. ROGGENBRODT: Okay.

5 MEMBER BROWN: So, an acceptance criteria  
6 for time response testing, okay, would be, because  
7 you've got a time response testing ITAAC somewhere. I  
8 vaguely remember that.

9 ME. ROGGENBRODT: Yes.

10 MEMBER BROWN: One of the metrics, and  
11 there may be others -- I mean that is just one that I  
12 picked up on, but that one, a time response test would  
13 not be, in my opinion, considered to be valid, if it  
14 was not done at that metric. You're saying, trust me.  
15 You're not saying that, but you're saying my  
16 expectation would be that that 70 percent would be  
17 reflected in the procedure. And my expectation is, if  
18 it is not specified in the DCD ITAAC acceptance  
19 criteria, or DAC, whatever the right thing is, there  
20 is a good chance they will run the test with whatever  
21 modules they've got in there, and if it passes, that's  
22 fine, but it's not at the design limit for where that  
23 platform is allowed to be operated.

24 ME. JACKSON: Right.

25 MEMBER BROWN: That's my only point. And

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 so, when we are talking about we are now out of the  
2 software process space and into an execution space, on  
3 all those topical reports, certain critical parameters  
4 that I would have expected to see make sure they got  
5 instituted were inserted into the test program  
6 eventually, when the procedures were written. That  
7 was the only purpose in my comment.

8 ME. JACKSON: I would say this with regard  
9 to that particular criteria, the 70 percent loading,  
10 that's in their DCD. If we found that they were  
11 testing it to some other criteria or not even testing  
12 it at all, then they would be in non-compliance  
13 with --

14 MEMBER BROWN: Let me go back to square  
15 one. The acceptance criteria, in the description and  
16 the test and the other things, critical elements --  
17 critical elements -- that some folks that have to  
18 agree that this design is satisfactory would expect to  
19 see that they don't slip through the crack would be  
20 specified either in the description --

21 ME. SANTOS: It is --

22 MEMBER BROWN: Let me finish, Dan. Okay?  
23 In the description or in whatever the second column  
24 is, I have forgotten what the title is, "test and"  
25 something, and then the acceptance criteria.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 Somewhere in there, they said, hey, what are the two  
2 or three specific items that have to be met, because  
3 they are the limits within which those platforms are  
4 supposed to be operated.

5 ME. SANTOS: Okay, you cannot take a DAC  
6 in isolation and run with it. It is the combination  
7 of the DCD and the DAC description, what is used to  
8 actually generate the DAC or the ITAAC procedures.

9 So our expectation is, for that particular  
10 item, okay, I have the criteria in the DAC. I go back  
11 to the DCD and pull out all the necessary details and  
12 put those in my inspection procedures. So, then, the  
13 inspectors and the experts go and look at that. That  
14 is one of them which you will be able to have in  
15 there.

16 CHAIRMAN BLEY: Charlie, I think you have  
17 made your point really well.

18 MEMBER BROWN: Go on. We need to move on.

19 CHAIRMAN BLEY: I want to point out that  
20 we are going to be going over the inspection  
21 procedures as you develop them and pass them on to us.

22 I, for one, will be looking to see how you can ensure  
23 these things are picked up in that procedure, if they  
24 are not laid out in the manner Charlie has laid before  
25 you here.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           And Bill was about to finish something  
2 before. Now I wanted to hear it.

3           ME. ROGGENBRODT: Well, I was just going  
4 to point out, you know, the expectation on our end is  
5 what we might see in a test procedure. But speaking  
6 to the point that was also raised, our mechanism to  
7 validate or verify this, which is what DAC is all  
8 about, is to say these are the criteria we would note  
9 in a forthcoming inspection procedure.

10           So you wouldn't just look at the DAC,  
11 which is very high-level in Tier 1. You would go into  
12 Tier 2 space. Then you would look into the secondary  
13 references, which are also part of the DCD. In this  
14 case, the report you are going to is the WCAP-16775 on  
15 the architecture.

16           Then you would have a technical expert  
17 from the staff go through that, comb through that  
18 report, and say, okay, here's some of my criteria.

19           CHAIRMAN BLEY: Let me just lay out --

20           ME. ROGGENBRODT: And say, within the  
21 inspection space, you would then verify it, match that  
22 to what they did in the procedure to find if it is  
23 acceptable or not.

24           CHAIRMAN BLEY: But kind of the problem we  
25 have, I think, is that's a lot of stuff you have to go

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 back and sift through.

2 ME. ROGGENBRODT: Correct.

3 CHAIRMAN BLEY: When the DAC are laid out,  
4 and now I will say it as if we were having a new  
5 design to come in, that seems like the place; it  
6 should have been combed through and organized into one  
7 place. Because having confidence that we will go back  
8 and find all of that at the end of the process, if it  
9 wasn't built in, is something that is, at least from  
10 where I sit, a little hard to see how we make sure  
11 that works.

12 Now, Said, you had something you wanted to  
13 bring forward?

14 MEMBER ABDEL-KHALIK: I just want to ask  
15 sort of a big-picture question. Specific details  
16 aside, in your view, is there any disagreement between  
17 the ACRS and the staff regarding the rigor or depth of  
18 the staff's review and/or ACRS's involvement in  
19 reviewing DCD amendments that provide details or  
20 detailed information leading to the closure of a DAC?

21 ME. SANTOS: Can you --

22 MEMBER ABDEL-KHALIK: Do you want me to  
23 repeat that?

24 ME. SANTOS: Yes, can you repeat that  
25 again before I answer it? I just want to make sure.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                    *MEMBER ABDEL-KHALIK: I will repeat it.*

2                    *Specific details aside, in your view, is*  
3 *there any disagreement between ACRS and the staff*  
4 *regarding the rigor or depth of the staff's review*  
5 *and/or ACRS involvement in reviewing DCD amendments*  
6 *that provide detailed information leading to the*  
7 *closure of a DAC?*

8                    *ME. SANTOS: From a technical standpoint,*  
9 *no.*

10                   *MEMBER ABDEL-KHALIK: So, in the past*  
11 *hour, you have essentially presented an example of a*  
12 *process that we both agree should work.*

13                   *ME. SANTOS: Correct. Option one,*  
14 *correct.*

15                   *MEMBER ABDEL-KHALIK: So the point here is*  
16 *what?*

17                   *MS. DUDES: I think it is illustrative*  
18 *because we are going to go into another example where*  
19 *a DAC remains, and then we are going to talk about the*  
20 *inspection process. And we are trying to just*  
21 *demonstrate to the Committee that the rigor associated*  
22 *with what goes on here will continue, regardless of an*  
23 *option that is chosen at a later date.*

24                   *MEMBER ABDEL-KHALIK: So the case will be*  
25 *made by inference?*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. DUDES: Yes. And I think, also, you  
2 know, one of the challenges, as I sit in many of the  
3 design-specific meetings that we have, is we have a  
4 very little amount of time to cover an enormous amount  
5 of information. So, we are trying to use this  
6 additional time where we can focus on really the depth  
7 and scope of these reviews and then make analogies to  
8 how this will progress, regardless of the regulatory  
9 option that is being used to resolve DAC.

10 So this was one where we used an  
11 amendment. I think we have had some good interactions  
12 and technical exchanges. We are also taking the  
13 opportunity to really expand upon the depth and scope  
14 of what we can share with the Committee in any given  
15 meeting.

16 So I think we will move on from that --

17 MEMBER ABDEL-KHALIK: Okay. So we will  
18 wait --

19 MS. DUDES: Yes.

20 MEMBER ABDEL-KHALIK: -- to see the rest  
21 of the presentation.

22 MS. DUDES: Yes. And I just want to say,  
23 because I don't think there will be too much lingering  
24 out there, we really want to try to capture as much as  
25 we can. And I hear the Committee's concern, and I am

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 going to articulate it, and I would like you to  
2 correct me.

3 We will move on, but correct me if I'm not  
4 getting this right. But there is an underlying  
5 concern about the general wording of the ITAAC in the  
6 design documents where you are not sure critical  
7 characteristics are going to be picked up at a later  
8 date because, although they may exist in the  
9 applicant's licensing basis, the process by which the  
10 staff would go back and capture that information and  
11 assure they are verifying critical attributes, maybe  
12 that is a concern that you were expressing in the past  
13 few minutes? Did I articulate that?

14 MEMBER BROWN: Yes.

15 ME. SANTOS: Is that it? Okay.

16 MEMBER BROWN: Yes.

17 MS. DUDES: Yes.

18 MEMBER BROWN: I mean, an example, in past  
19 programs we used to have a procurement staff. We did  
20 stuff and we articulated all types of requirements.  
21 Then we had a set of test requirements where we came  
22 back and we said, okay, and we either quoted the  
23 sections and said you now have to do this to  
24 demonstrate A, B, blah, blah, blah, and on down.

25 MS. DUDES: Okay.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   **MEMBER BROWN:** Down here, you've got 500  
2 *pages worth of stuff, a lot of things buried all over*  
3 *the place, little details, some of them only*  
4 *articulated by being explained in some of the*  
5 *meetings, and the nuances are not captured in the DCD.*

6                   *You know, we haven't asked for specific revisions in*  
7 *many circumstances. They are captured either in*  
8 *minutes or other discussions, RAIs, et cetera.*

9                   *And you all argued, not argued,*  
10 *articulated -- let me use that word.*

11                   *(Laughter.)*

12                   *I am not trying to be pejorative here.*

13                   **MS. DUDES:** No, I know that.

14                   **MEMBER BROWN:** Articulated that all of  
15 *those are used as part of the licensing basis, once*  
16 *the certification is granted. So, for the neophytes*  
17 *like myself, okay, I buy in on that, but still that is*  
18 *a lot of stuff.*

19                   *But there are certain critical attributes*  
20 *which you have heard me articulate many times to this*  
21 *point that you need to focus on from a top-level*  
22 *standpoint and make sure those things get covered, and*  
23 *then let process, which you have to have, pick up*  
24 *loose ends, the smaller pieces. But you need to cover*  
25 *the big stuff and make sure that is covered and clear;*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you have the independence to determine as in blah,  
2 blah, blah, et cetera, et cetera.

3 So, anyway, that's --

4 MS. DUDES: Right, and I appreciate that,  
5 because we are getting down to, okay, we make a safety  
6 finding in the DCD, but this is good feedback for  
7 something that is actionable and that we can continue  
8 to work on in terms of how do we capture that concern.

9 Because I think the staff over time has looked at a  
10 lot of documents and said, yes, it's in there; yes,  
11 it's in there. And that may not be a satisfying  
12 answer.

13 I hear what you are saying. So we need to  
14 continue to work. I am just trying to narrow down the  
15 concerns.

16 MEMBER BROWN: It is both. And it is not  
17 just DAC. It's ITAAC and DAC.

18 MS. DUDES: Yes, I agree.

19 MEMBER BROWN: For example, you can go  
20 look at the ITAAC on some of these where they want to  
21 check the bypass switches. They go and they turn this  
22 switch, and they check the bypass and see that it  
23 bypasses it, and the function no longer operates.  
24 That works. That is a nice, clear, crisp acceptance  
25 criteria.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. DUDES: Okay.

2 MEMBER BROWN: I quit for this one --  
3 maybe, for a while, a few minutes.

4 (Laughter.)

5 ME. JACKSON: Well, I mean we understand  
6 your concern and I understand what you are saying.  
7 You would like to see more specific criteria within  
8 the ITAAC itself rather than its being captured in the  
9 DCD somewhere.

10 MEMBER BROWN: Not every one of them.  
11 There's no way --

12 ME. SANTOS: The critical ones.

13 MEMBER BROWN: The certain critical ones,  
14 okay, and I can name other ones, but I want you to go  
15 ahead and finish.

16 ME. JACKSON: And I guess what the staff  
17 is maybe saying is that we have the regulatory tools.  
18 I mean this might be getting into process, but we  
19 have the regulatory tools to ensure that those  
20 critical characteristics, as well as others, are in  
21 the DCD, that they are actually implemented in the  
22 appropriate way.

23 I know that I don't want to belabor the  
24 point, but --

25 MEMBER BROWN: Since Dennis, the Chairman,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *Mr. Chairman, since you said we had some time, I will*  
2 *provide one other.*

3 *AP1000 uses the high-speed links. They*  
4 *also use -- correct me -- the dual-port RAM. And the*  
5 *argument is between the CRCs or whatever they use from*  
6 *the date of validation from point A to point B, the*  
7 *dual-port RAM is quote, "an excellent isolation*  
8 *device" and will allow no nasty stuff to go from a*  
9 *processor off to a voting unit. You all made that*  
10 *statement, maybe in slightly different terms, but that*  
11 *is the independence. That has provided the isolation*  
12 *on the data side, the CRC and the dual-port RAM.*

13 *Now you go look, where is the test, okay,*  
14 *an ITAAC, that takes data, because it is a field of*  
15 *data for a high-speed link. I mean there's headers*  
16 *and footers and stuff in between, or whatever, that*  
17 *gets stripped out in various places. And you send a*  
18 *variety of different types of good data and bogus data*  
19 *into that thing and see that nothing gets through, and*  
20 *that the bad stuff doesn't get through and the good*  
21 *stuff does. There's no ITAAC for that. It is just*  
22 *there.*

23 *Okay. Now so it is a critical attribute*  
24 *for independence. So I would expect to see some type*  
25 *of test description that says you test it over a range*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *suitable such that you demonstrate that no bad stuff*  
2 *gets through and all the good stuff does.*

3 *Now I may be saying that not as eloquently*  
4 *as I could because I'm not a software geek. Okay?*

5 *ME. JACKSON: Let me maybe respond.*

6 *MEMBER BROWN: I don't want you to -- I'm*  
7 *not sure, do you want him to really answer this one*  
8 *right now?*

9 *(Laughter.)*

10 *That's just an example of something that*  
11 *is expected you would see in a test --*

12 *ME. JACKSON: But I don't want to*  
13 *necessarily leave things out on the table, either.*

14 *MEMBER BROWN: Right.*

15 *ME. JACKSON: And I will ask the*  
16 *Westinghouse representatives in the audience, if I*  
17 *begin to get into proprietary space, to let me know.*

18 *But what you have described there about*  
19 *the dual-port RAM, that is one part of the data*  
20 *communications independence.*

21 *MEMBER BROWN: Yes.*

22 *ME. JACKSON: There's other aspects that*  
23 *are also critical to overall independence with regards*  
24 *to data communications independence. And then,*  
25 *independence overall includes some other aspects as*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 well.

2 MEMBER BROWN: Okay. If they are listed  
3 in the DCD, Terry, they ought to be listed in the  
4 acceptance criteria that they are verified. That's  
5 the point.

6 ME. JACKSON: And that is what we  
7 understand is --

8 MEMBER BROWN: And that's not there right  
9 now.

10 CHAIRMAN BLEY: I think we have beat on  
11 this enough. I'm going to turn it back to you, with  
12 one little thing. There may be three things that have  
13 come out in the discussions, not just today, but  
14 previously, with respect to this.

15 One is the technical issue of these  
16 acceptance criteria, both ITAAC and DAC, and the  
17 criteria aren't complete there. Now, if things are in  
18 the DCD, you have got to meet them, if they are things  
19 you have to meet. And having confidence that those  
20 are all picked up and how you are going to get to that  
21 is something we want to understand.

22 There is another issue that has been  
23 raised. And that is, many of the V&V and everything  
24 is to ensure that the system does those things it is  
25 supposed to do.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           And the other side of systems analysis for  
2 everything is to say, gee, are there unusual  
3 conditions under which it might do something it  
4 shouldn't do? And we are having trouble seeing where  
5 those are covered. So we would like to hear more  
6 about that piece of it.

7           And the last one is the one we talked  
8 about in that informal meeting, which if these are the  
9 acceptance criteria, and that's what they're called,  
10 and you get post-COL to a point that someone says,  
11 "Here's the criteria and I've met it, and I don't want  
12 to do anything more," how do we get that resolved? So  
13 that is an issue that is of some concern where the  
14 onus is back on you.

15           And maybe Charlie's example of the 70  
16 percent load is one where you say, well, I want to see  
17 it loaded at 70 percent; it doesn't say it here,  
18 though.

19           So those are the three things, not to  
20 address right now, but just to leave you with those.

21           ME. JACKSON: Okay.

22           CHAIRMAN BLEY: And I would say, back to  
23 you, Terry, to finish up.

24           ME. JACKSON: Okay. And I think maybe to  
25 your first point, I will try to address that a little

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 bit. That is that I think that is the concern that  
2 I&C staff has when we are reviewing as well as when we  
3 are auditing or inspecting. It is you want to make  
4 sure the system does what it should do and it doesn't  
5 do what it shouldn't do.

6 Part of that, if I go back to the  
7 requirements specification, that was part of what we  
8 were looking at, I mean one part: how does the system  
9 respond to conditions that weren't anticipated?

10 So, for example, in some cases they can  
11 put requirements in and say we're going to limit the  
12 dataset to this dataset. Everything else is going to  
13 be alarmed or take some action. If they don't have  
14 that, then we question and we say, well, what happens  
15 if this occurs? So that is kind of the level of  
16 detail that we get to.

17 It is hard to demonstrate it here because  
18 it is not on paper per se, but it is part of the  
19 discussion, part of the document review that we do  
20 when we are on audits or when we are on inspections.

21 **MEMBER ABDEL-KHALIK:** If I may follow up?

22 **CHAIRMAN BLEY:** Yes.

23 **MEMBER ABDEL-KHALIK:** To finally follow up  
24 on my sort of big-picture question, a comment was made  
25 that the purpose of this part of the presentation was

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to illustrate the depth and rigor of the review  
2 process. And the inference is that you will continue  
3 the same level of depth and rigor in inspection  
4 processes for review of DAC post-COL, absent ACRS  
5 review.

6 Now this process, we both agree, is  
7 successful because it provides the depth and rigor and  
8 oversight that would assure the appropriate system  
9 design that meets whatever criteria we set out to do.

10 Now you are implying that, if you do your part to the  
11 same level of depth and rigor without any input from  
12 ACRS, that you would achieve the same objective for  
13 inspection-type processes. Is that a correct problem  
14 definition?

15 ME. SANTOS: No, I will say that we  
16 together and your oversight, the staff and the  
17 oversight provided by the ACRS help us reach a safety  
18 finding that the design, it is safe and it meets our  
19 regulation.

20 And all we are doing, whether it is  
21 closing a DAC or an inspection ITAAC, is verifying  
22 that the implementation of that safe design meets the  
23 design basis or licensing basis that we collectively  
24 and your oversight reviewed.

25 MEMBER BROWN: You missed the point.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. DUDES: Well, you know, I would like  
2 to see if we can keep moving on. I clearly understand  
3 your point, and I think that was articulated in your  
4 letter as well. I think that that is something that  
5 we are going to take on in probably a different form,  
6 because I don't really want to put the staff in the  
7 position to make that call up there right now. I  
8 would prefer to just keep going.

9 CHAIRMAN BLEY: Okay. Go ahead, please.

10 ME. SANTOS: Mr. Chairman, I do understand  
11 your point. I elected to --

12 MEMBER ABDEL-KHALIK: No problem.

13 ME. SANTOS: I elected to express it that  
14 way.

15 MEMBER ABDEL-KHALIK: No problem.

16 ME. JACKSON: Okay. Let's go to the next  
17 slide, Dan, and the next one after that. Actually,  
18 okay, future efforts.

19 So what we wanted to describe here was the  
20 future efforts. So, as we are just talking about, we  
21 are saying that same level of effort will be applied  
22 to future technical and process information received  
23 related to amended design certifications and license  
24 reviews.

25 So, for example, we mentioned that the CIM

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 development process DAC was still going to remain.  
2 And Westinghouse is expected to provide a more robust  
3 development process.

4 The staff, once that is completed, then we  
5 will use the same types of audit-type activities to  
6 verify that as we did previously. So, if this is in  
7 inspection space where, say, a combined license  
8 applicant has a license and they are doing this post-  
9 COL, we are going to do the same activities as we did  
10 in the audit, where we identified the original issues.

11 The same thing with the system definition  
12 phase. We will do the same types of activities as we  
13 did in those audits, but that will likely be in  
14 inspection-type format.

15 And then, finally, technical agency  
16 experts from I&C, the Construction Inspection staff,  
17 and other technical experts will continue to use them  
18 to support the review, whether it is the review audit  
19 inspection process for DAC resolution and closeout  
20 effort.

21 Then, in conclusion, we feel that we  
22 performed an in-depth evaluation of vendor engineering  
23 documents to verify the resolution and closeout of  
24 DAC/ITAAC material and that we will address non-  
25 compliance as necessary.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1                   Acceptance criteria, review tools,  
2                   technical report review, and level of effort for  
3                   inspections are similar to those used in audits during  
4                   design certification and license reviews.

5                   The inspection activities are similar to  
6                   what occurred during the audit activities. One thing  
7                   I wanted to mention is there is little differentiation  
8                   between the DAC and ITAAC. DAC is an ITAAC.

9                   MEMBER ABDEL-KHALIK: I'm sorry, have you  
10                  demonstrated that so far, that second bullet?

11                  ME. JACKSON: The sub-bullet under the  
12                  second bullet or the overall second bullet itself?  
13                  The acceptance criteria, review tools, technical  
14                  report? I think we will cover that in the later  
15                  presentation, when we get to the inspection part.

16                  But, I mean, I am kind of speaking from my  
17                  experience because I was an inspector for seven years  
18                  and I'm familiar with the inspection process. So,  
19                  when we did the audits that we did at Westinghouse, we  
20                  actually formed the teams and arranged the activities  
21                  similar to an inspection activity, mainly because we  
22                  knew that it was a format and a process which had been  
23                  used and was successful in the past. Plus, I wanted  
24                  to give my staff some experience at doing a similar-  
25                  type process, so if they are called upon to help out

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in an inspection later on, they would at least be  
2 familiar with the process.

3 So, I would say, yes, we do have some  
4 experience because our audits were structured, that we  
5 conducted in this particular example were structured  
6 similar to what would occur in an inspection.

7 MEMBER ARMIJO: Terry, your use of the  
8 word "similar" is what bothers me. I would like to  
9 see that word to be "are equivalent". They have to be  
10 to the same level, the same depth, the same quality  
11 before I can start feeling confident that they aren't  
12 just something of lesser --

13 ME. JACKSON: Right. I think,  
14 technically, they are the same. Because, for example,  
15 if --

16 MEMBER ARMIJO: I would like to see you  
17 put up charts that say, "We believe these are going to  
18 be equivalent."

19 ME. JACKSON: Okay.

20 MEMBER ARMIJO: And maybe you are. When  
21 you use a word "similar", it is kind of --

22 ME. SANTOS: Right. Good comment. I know  
23 the folks who are in inspections, if you can --

24 MS. DUDES: Why don't we just keep at it  
25 because we do have a whole presentation on inspections

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and we plan to do that?

2 ME. SANTOS: Yes.

3 MS. DUDES: So Tom can talk to that when  
4 he comes on.

5 ME. JACKSON: Okay. And so, my final  
6 point is that, well, I did make that. You know, the  
7 technical agency experts will be on hand to help out  
8 in the inspection process.

9 So that concludes our presentation for the  
10 AP1000 example.

11 ME. SANTOS: Are there any questions?

12 CHAIRMAN BLEY: Okay. And the rest of  
13 this package are just things you did use?

14 ME. JACKSON: Right.

15 CHAIRMAN BLEY: Thank you.

16 Anything else from the members?

17 (No response.)

18 It looks like we are at least more than  
19 half through the slides that were brought. We had a  
20 break scheduled for 3:00. I'm thinking this would be  
21 the appropriate time to take it.

22 No one objects? Okay, we will recess for,  
23 I'm going to be generous, 18 minutes. Be back here;  
24 we'll start promptly at three o'clock.

25 We're off the record until then.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   *(Whereupon, the foregoing matter went off*  
2 *the record at 2:42 p.m. and went back on the record at*  
3 *3:00 p.m.)*

4                   *CHAIRMAN BLEY: We are back in session,*  
5 *please.*

6                   *The recorder is online, okay.*

7                   *Who's up?*

8                   *Okay, Mr. Jung.*

9                   *ME. JUNG: Good afternoon.*

10                  *My name is Ian Jung, Chief of the*  
11 *Instrumentation, Controls, and Electrical Branch No.*  
12 *2, just a counterpart to Terry Jackson, who made a*  
13 *presentation earlier.*

14                  *I would just note that, for those who are*  
15 *listening to this call, the set of slides that Thomas*  
16 *Fredette is going to present regarding ITAAC/DAC*  
17 *inspection is actually a part of our set of ESBWR*  
18 *slides, since it is a followup to a very specific*  
19 *example regarding single-failure criteria associated*  
20 *with the ESBWR design.*

21                  *So, along with me is Dinesh Taneja. He is*  
22 *the Senior Electronics Engineer. And then, Kimberly*  
23 *Corp, my staff, and Dan Santos is the senior-level*  
24 *advisor to the Division.*

25                  *Just for introduction, most of the*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 presentation is going to be done by Kimberly and  
2 Dinesh. I just want to introduce at a higher level  
3 what ESBWR review meant to the staff from an I&C  
4 perspective.

5 It has been about five years of review.  
6 The staff spent more than 15,000 hours of review for  
7 ESBWR design certification, and about 300 requests for  
8 additional information, which does not include many of  
9 the actually supplemental RAIs.

10 And we had numerous interactions not only  
11 with the ACRS, but public meetings, closed meetings,  
12 and a lot of public meetings with the GEH regarding a  
13 number of safety issues, a number of not necessarily  
14 safety issues, but regarding what is the licensing  
15 basis information we need to have as well as deciding  
16 on whether DAC or ITAAC, what are the level of  
17 specifics that are in the DAC, you name it. It has  
18 been a tremendous effort from the staff's perspective.

19 In addition to Chapter 7, we were involved  
20 in many other chapters that I&C is part of the overall  
21 safety design. We spent quite a bit of additional  
22 hours related to Chapter 3, 6, 8, 9, 10, 11, 14, 15,  
23 16, 18. We didn't accrue all the number of hours we  
24 spent on those non-Chapter 7 hours.

25 Looking back, Revision 1 through Revisions

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 all the way to 8, the difference in licensing basis  
2 and safety improvements made in the ESBWR design is  
3 tremendous.

4 On licensing basis information, we have  
5 come to agreement with GEH was about 1,250 pages, in  
6 the approximate range, for Chapter 7.

7 Today we have worked with the Christina  
8 Antonescu regarding what example we want to present  
9 the Committee with. We just decided to go with a  
10 single-failure criterion, which is IEEE 603-5.1.  
11 There could have been other good examples, but we felt  
12 this is one relatively simple example, but it also  
13 deals with a very important design criteria, not for  
14 electrical I&C, for mechanical systems. They all use  
15 single-failure criteria as one of the key acceptance  
16 criteria for safe design.

17 We hope to achieve providing the Committee  
18 regarding the steps, reviews, scope, the depth and  
19 level of resources we spent on this, and how we came  
20 to the safety decision regarding this, along with the  
21 DAC, how we came to the DAC to be acceptable, how we  
22 envision the DAC to be resolved down the road.

23 Specifically, on this single-failure  
24 criterion, overall, the staff found that the Tier 2  
25 DCD contained sufficient information to make a safety

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *finding. And staff evaluated with a sufficient level*  
2 *of depth and detail and scope to reach the safety*  
3 *finding, and DCD Tier 1 information is found to be*  
4 *acceptable and provide the opportunities for adequate*  
5 *verification of detailed implementation of the Tier 2*  
6 *design information.*

7 *Other areas of DCD also provide a defense-*  
8 *in-depth and overlaps regarding overall safety design.*

9 *Because if you just look at the single-failure*  
10 *criterion, meeting that particular criterion doesn't*  
11 *necessarily provide a sufficient overall plant safety.*

12 *So you have got to look at the overall IEEE 603*  
13 *criterion. There are dozens of others.*

14 *Some of those are very interrelated to*  
15 *single-failure criterion. There is a redundancy in*  
16 *their independence. But we are not going to go to*  
17 *those areas specifically because those sections are*  
18 *also addressed separately in here, too. But you*  
19 *cannot separate them in a very clean way from each*  
20 *other.*

21 *So, with that in mind, we want to go back*  
22 *to sort of single-failure criterion to focus on it,*  
23 *because the goal of our presentation is to provide you*  
24 *with information surrounding single-failure criterion,*  
25 *what it means from the perspective of that ITAAC, and*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the level and scope of the staff review.

2 So, with that, I will turn it over to  
3 Kimberly Corp, who is going to do an initial set of  
4 slides. Then, Dinesh is going to go through more  
5 technical details.

6 MS. CORP: Good afternoon.

7 As Ian stated, we have provided this  
8 example because we felt the single-failure criterion  
9 showed the integral part of the overall plant design  
10 from its scope, level of depth, detailed depth, and  
11 breadth, not only in the DCD, but as well as in the  
12 staff review.

13 Our presentation will go through  
14 definition of the single-failure criterion, the safety  
15 issues, significant findings that we had for the  
16 single-failure criterion, as well as the requirements  
17 and guidance used by the staff for its review.

18 Then, Dinesh will delve deeper into the  
19 Tier 1 and Tier 2 information from our example, as  
20 well as the staff review of that information, and then  
21 explain how we found the DAC to be of quality and  
22 acceptable.

23 And then, Thomas Fredette will go into the  
24 DAC inspection and ITAAC inspection.

25 Just quickly, the definition straight from

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *IEEE 603: The safety systems will perform; with any*  
2 *single detectable failure concurrent with all*  
3 *identifiable, but non-detectable; all failures caused*  
4 *by the single failure, and all failures and spurious*  
5 *system actuations that cause, or are caused by, the*  
6 *design basis event requiring that safety function.*

7 *Next slide.*

8 *Safety failure criterion is very important*  
9 *to overall safety, so that the design can cope with a*  
10 *single failure. It is significant because it protects*  
11 *against a single failure, ensuring a highly-reliable*  
12 *and functional safety system through independence and*  
13 *redundancy.*

14 *The staff found, and it was presented to*  
15 *the ACRS I think last week, with the Design Center for*  
16 *ASBWR, that the I&C system was designed with*  
17 *sufficient redundancy and independence; that the DCD*  
18 *described in detail that the design complies with the*  
19 *single-failure criterion, and, in addition, that the*  
20 *DCD includes a detailed, well-structured methodology,*  
21 *as well as a set of DAC and ITAAC that ensures a high-*  
22 *quality translation of the licensing basis into the*  
23 *detailed implementation that staff found to be*  
24 *acceptable.*

25 *Next slide.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           The requirements that the staff used is 10  
2 *CFR 50, Appendix A, particularly GDCs 21 and 23, as*  
3 *well as 10 CFR 50.55a(h), which is IEEE 603,*  
4 *particularly Clause 5.1, single-failure criterion.*

5           The staff used for guidance the Standard  
6 *Review Plan as well as IEEE 7-4.3.2, and particularly*  
7 *for the single-failure criterion, the Reg Guide 1.53,*  
8 *which endorses IEEE 379, application of the single-*  
9 *failure criterion to nuclear power plants.*

10           *Next slide.*

11           *Just to show you that all safety systems,*  
12 *including I&C, are required to comply with the single-*  
13 *failure criterion. As you can see, six GDCs also*  
14 *specifically address that their safety systems need to*  
15 *comply with the single-failure criterion.*

16           *Also, IEEE 603, Section 5, "Safety System*  
17 *Criterion", the single failure is just one of the 15*  
18 *clauses that the staff reviewed.*

19           *Also, single-failure criterion is evident*  
20 *throughout the entire life cycle process.*

21           *Next slide.*

22           *The single-failure criterion is, again,*  
23 *integrated in the overall DCD. The redundancy and*  
24 *independence is not only addressed at the division*  
25 *level, but in the system level, and sometimes even*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 drilled down into the logic and component level as  
2 well.

3 The life cycle process, each safety system  
4 implements it, and the DAC and ITAAC are resolved in  
5 the life cycle.

6 The single-failure criterion was  
7 referenced over 250 times within the Tier 1 and Tier 2  
8 information for digital I&C.

9 And now Dinesh will go into the specific  
10 example documentation.

11 ME. TANEJA: Thanks, Kimberly.

12 I am Dinesh Taneja.

13 We reviewed the ESBWR design quite  
14 extensively. In the example that we have chosen, the  
15 single-failure criteria, this table 2.2.15 comes from  
16 Tier 1. This is the table that provides like a  
17 summary of the compliance to all of the IEEE clauses.

18 I think the one we are highlighting is 5.1, which is  
19 the single-failure criteria.

20 As it can be seen, all safety systems  
21 implemented in the Q-DCIS complied with the single-  
22 failure criteria Clause 5.1 of IEEE 603. The single-  
23 failure design feature compliance will be documented  
24 in the 603 Clause 5.1 compliance report, and that is  
25 the "R" that is indicated there.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           There will be seven compliance reports,  
2 one per each software project. And the seven software  
3 projects are implemented on three separate diverse  
4 platforms.

5           MEMBER BROWN:     What is the difference  
6 between "C" and "R" again? I missed that.

7           ME. TANEJA:     Like there are seven software  
8 projects. RTIF, for example, is one of the software  
9 projects.

10          MEMBER BROWN:    All the ones labeled "R"  
11 are software projects then? Is that what you are  
12 saying?

13          ME. TANEJA:     Well, "R" is a report. Okay?  
14 They all comply. All of the safety systems comply.  
15 What "R" means is that there is that report which  
16 contains -- the "Cs" to the right of it within that  
17 report, for compliance to that specific criteria.

18          So, that software project report, there  
19 would be one report for that software project, which  
20 is to demonstrate compliance of these other safety  
21 systems, planned safety systems designed to be in  
22 compliance with that same IEEE criteria.

23          So this is how they presented the  
24 information. So, you know, if you look at it, there  
25 are seven separate projects that are identified, RTIF,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 NMS, SSLC/ESF, you know, the vacuum break isolation  
2 function, ATWS, and the high-pressure CRD isolation,  
3 and the ICS. So these seven software projects, each  
4 will have a report. Okay? That will demonstrate  
5 compliance with the IEEE 603 criteria.

6 Now within these reports would be the  
7 plant safety systems. That would be demonstrated as  
8 complying to the same criteria. So I would take the  
9 example, see RTIF, the report would have the RPS  
10 system, the isolation system, nuclear boiler system,  
11 controller drive system, et cetera. That's what it  
12 means.

13 MEMBER BROWN: Software projects?

14 ME. TANEJA: Software project --

15 MEMBER BROWN: Is it just the software?  
16 What do you mean by that?

17 ME. TANEJA: Okay. What this means is  
18 that ESBWR design uses three different platform  
19 technologies. Okay? There would be an RTIF/NMS  
20 platform; there would be an SSLC/ESF platform, and the  
21 ICP platform, right?

22 MEMBER BROWN: Uh-hum.

23 ME. TANEJA: Now the software project is  
24 like designing one set of software package that will  
25 run on that platform. So there would be separate

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 software projects that would be designed. The life  
2 cycle processes that would be followed would be  
3 followed seven times.

4 MEMBER BROWN: Okay. Where is the  
5 hardware design analyzed for single-failure?

6 ME. TANEJA: I'll come to it.

7 MEMBER BROWN: You'll come to it? Okay.

8 ME. TANEJA: I'll come to it.

9 CHAIRMAN BLEY: So this is strictly  
10 software?

11 MEMBER BROWN: This is strictly software.

12 CHAIRMAN BLEY: In other meetings, some of  
13 you have always said, "Gee, we used `software', but it  
14 means the whole system." But here we're talking  
15 straight software?

16 ME. TANEJA: Well, the thing is the  
17 software development is actually covered under 3.2,  
18 ITAAC, under Tier 1, Section 3.2. It addresses the  
19 entire software development process, and there are  
20 DACs in there for that. Okay?

21 This specifically talks to compliance of  
22 the IEEE 603 criterias. Okay? They are all  
23 overlapping.

24 Now the hardware comes in under the  
25 systems. Okay, so if I look at, for example, the Tier

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 documentation, the I&C is under 2.2 of Tier 1,  
2 right? 2.2.7 is RPS. So I have ITAACs and design  
3 descriptions for RPS in 2.2.7. They are all  
4 overlapping.

5 I mean we have multiple ways. There are  
6 all kind of matrices vertically and horizontally that  
7 tie all of them together.

8 So, when we look at one little piece of  
9 it, that is one opportunity, but we have multiple  
10 opportunities of inspecting, reviewing, and verifying  
11 all these things.

12 MEMBER RYAN: Dinesh, one question. You  
13 made a good point. How do you verify to yourselves,  
14 in doing that review process, that you looked at all  
15 the combinations that can get you to a problem?

16 ME. TANEJA: Right.

17 MEMBER RYAN: I think when Charlie was  
18 asking questions earlier, I get the sense that is what  
19 he was reaching for.

20 ME. TANEJA: Right.

21 MEMBER RYAN: How do you assure yourself  
22 that you have looked at all important, at least, if  
23 not all, of those connections through that matrix that  
24 you just described?

25 ME. TANEJA: Well, see, that's one thing.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1       You know, I&C discipline is not just limited to the  
2 I&C. I&C, you know, we basically have to understand  
3 Chapter 13 for us to know what functions are  
4 considered safety functions, to be able to say that  
5 you have taken care of the critical features.

6               We have to understand the RPS system. So  
7 we have to be into Chapter 5 and Chapter 6. ESF  
8 system, you have to understand, you know, what modes  
9 of operation that these equipment need to operate  
10 under and how they operate.

11               I&C, I consider I&C to be a support system  
12 which actually supports all the safety functions that  
13 a plant system needs to provide. So, when we look at  
14 I&C, Chapter 7 laid out, you know, 7.1 is a general;  
15 7.2 is RPS; 7.3 is ESF.

16               So, when we look at 7.2, for example, RPS,  
17 right, that has links to the reactor protection system  
18 that is described at a system level in Chapter, I  
19 think, 5 and 6. Then, Tier 1 actually summarizes what  
20 is in Tier 2, and it provides the relative ITAACs and  
21 DACs, right. So it is not a very simple review.

22               That is why, when Ian mentioned we spend  
23 so many hours, that is where these hours go.

24               MEMBER RYAN: Oh, no, I appreciate all  
25 that.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           ME. TANEJA: Right.

2           MEMBER RYAN: But I am trying to ask  
3 about, once you have been through that process --

4           ME. TANEJA: Right.

5           MEMBER RYAN: -- how do you determine  
6 you're in closure for the process? When do you say,  
7 "I'm done."?

8           ME. TANEJA: Okay. Let me say, our  
9 guidance primarily comes from the SRP 0800, which  
10 basically tells us, you know, okay, what are the  
11 acceptance criterias. And BTP 7-14 speaks to the  
12 software development life cycle in Chapter 7, and the  
13 Chapter 7 0800 SRP, the staff review guidance,  
14 provides us with a roadmap of how we want to do the  
15 reviews.

16          ME. SANTOS: So your point is -- Dan  
17 Santos now --

18          MEMBER RYAN: Still in the review process,  
19 though, Dinesh, I'm fine. I understand that there is  
20 a process. There is kind of a complicated layout, but  
21 I want to know, when do I know I'm done?

22          ME. TANEJA: Done with the safety finding?

23          MEMBER RYAN: Yes.

24          ME. TANEJA: Done with safety finding?  
25 Well, the safety finding --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           **MEMBER RYAN:** *In any one case, in any one*  
2 *example, when does the endpoint come?*

3           **ME. TANEJA:** *Okay. Well, the SER is where*  
4 *we document our findings. Okay? When we are done, it*  
5 *is that the compliance to the regulation is our review*  
6 *objective. Our objective is, does the design comply*  
7 *with all the regulations? 603 is the primary*  
8 *regulation, okay, for the I&C systems, and then it has*  
9 *the compendium GDCs that tie into it, right?*

10           **ME. TANEJA:** *And the way the SRP 0800 is written, it*  
11 *basically provides you with the guidance on, okay,*  
12 *these 603 criterias apply for this function. These*  
13 *GDCs apply for this function. So, when we are looking*  
14 *at a specific design, we are saying, okay, does it*  
15 *meet that criteria, design criteria? Does it meet*  
16 *that design feature that is in 603?*

17           **ME. TANEJA:** *I could say very easily I wish there was a*  
18 *checklist that I could go and I could check off --*

19           **MEMBER RYAN:** *Oh, no, no, no, I*  
20 *understand.*

21           **ME. TANEJA:** *-- but there is really no*  
22 *checklist.*

23           **MEMBER RYAN:** *I think it is important to*  
24 *recognize it is not going to be, because all these*  
25 *things are interrelated in ways --*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           ME. TANEJA: Right.

2           MEMBER RYAN: -- and probably a hundred  
3 others that you have just described.

4           ME. TANEJA: Right.

5           MEMBER RYAN: So, the point is, at some  
6 point, you are shifting from a checklist or making  
7 sure things are in the right place at the right time  
8 with the right specifications to --

9           ME. TANEJA: Right.

10          MEMBER RYAN: -- you're making a judgment  
11 of how it is going to work.

12          ME. TANEJA: Right. Correct.

13          MEMBER RYAN: That is the part I am trying  
14 to understand, is, when do you step off and start  
15 making judgments, and what do you use to make those  
16 judgments?

17          ME. TANEJA: There is engineering  
18 expertise that gets into play, and the experience that  
19 we have from maybe the existing operating plant fleets  
20 and the lessons learned, and then, also, we do  
21 interface with other regulators.

22          MEMBER RYAN: Sure. And an earlier  
23 speaker made the point that he was an inspector for a  
24 number of years.

25          ME. TANEJA: Ian and I, we went out to

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Korea and we looked at their digital designs, and we  
2 talked to them about their lessons learned, and where  
3 were the weaknesses, where were the strengths. We  
4 took that information. These are the insights that  
5 you have to kind of reach out to, to be able to do  
6 these reviews, you know.

7 ME. JUNG: Mr. Ryan, for an ESBWR case,  
8 the lead reviewer, Herbert Lee was the principal  
9 reviewer all by himself, I think, for AP1000 design  
10 certification, Revision 15. Also, he was involved in  
11 the previous remaining three certifications that has  
12 been certified by the agency, which helped him take  
13 the lead, also train the staff.

14 And our SRP Chapter 7, which is about this  
15 big, which references this much of IEEE standards and  
16 Reg Guides, all together provides rather prescriptive  
17 review criteria that staff needs to verify.

18 MEMBER RYAN: So that is an important  
19 point, I think, at least for me. Maybe it helps  
20 others, too.

21 But if you have very prescriptive criteria  
22 that you have derived from, first, your study of a  
23 design and an application, and all the rest of it, as  
24 well as your experience, and you are saying, in order  
25 to make the determination this is okay, you have to

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 really find these five or six elements to say, yes,  
2 that's okay, something like that?

3 ME. JUNG: Right. Yes.

4 MEMBER RYAN: I am just trying to get the  
5 process in my head.

6 ME. JUNG: Yes, certain sections of the  
7 SRP actually have a sample template SER. You have to  
8 make these safety conclusions in your SER. Especially  
9 RPS, for example, for GDC 23 requirements, you have to  
10 design a system to deal with the potential failure  
11 modes. You have to have a design to guarantee  
12 failsafe design.

13 So, failsafe design for RPS for 7.2, you  
14 have got to have a fail trip condition design built  
15 into your system, stable going into the design, and  
16 verify that there is such a design in place in DCD.

17 MEMBER RYAN: I guess I would defer to the  
18 Subcommittee Chairman and ask at some point it might  
19 be helpful to see a more detailed example of that  
20 thought process and how you went through all that, to  
21 understand how it works for you.

22 ME. JUNG: Hopefully, we like to achieve  
23 that, at least partially, through single-failure  
24 criterion today for this example.

25 MEMBER RYAN: Okay, but maybe there will

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *be some followup based on that presentation.*

2 *Thank you.*

3 *MEMBER BROWN: Just before you leave that*  
4 *chart --*

5 *ME. JUNG: Okay.*

6 *MEMBER BROWN: This is software, and I*  
7 *mean I don't think I'm right when I --*

8 *ME. JUNG: Mr. Brown, I think when*  
9 *somebody says "software" --*

10 *MEMBER BROWN: He said this was the*  
11 *software development life cycle. Those were the words*  
12 *used.*

13 *ME. TANEJA: Well, see, you know, we --*

14 *MEMBER BROWN: I can't handle much. Okay?*  
15 *It either is or it is not.*

16 *ME. TANEJA: It's not just software. It*  
17 *can never be a software. Software has to run on a*  
18 *machine.*

19 *MEMBER BROWN: I'm just trying to get an*  
20 *answer.*

21 *ME. TANEJA: It doesn't exist in a vacuum,*  
22 *right?*

23 *MEMBER BROWN: I don't disagree, but, I*  
24 *mean, I almost walked away with saying, gee, you're*  
25 *doing a software single-failure criterion review --*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   ME. TANEJA: No.

2                   MEMBER BROWN: -- and I know you're not  
3 doing that.

4                   ME. TANEJA: Software projects, okay, RTIF  
5 and NMS software projects, they are two software  
6 projects that are implemented on the RTIF/NMS  
7 platform. When we say "platform", that is hardware.  
8 Okay? When we say "RTIF software project", it is the  
9 application, the RTIF application running on that  
10 platform. So that is one application.

11                   Another application would be an NMS  
12 application. So that is another software project that  
13 runs on a similar platform. I mean not similar. The  
14 same boxes, the same design, the same, but on a  
15 separate box.

16                   MEMBER BROWN: A separate platform, a  
17 different computer?

18                   ME. JUNG: A separate box.

19                   ME. TANEJA: In this case, I think the  
20 intent is to use NUMAC, right? So there is a NUMAC  
21 box for the RTIF platform or application, and there is  
22 a NUMAC box for the NMS. Okay?

23                   ME. JUNG: Similarly, the whole purpose of  
24 this slide is how single-failure criterion is  
25 separated out and applied in all safety systems. That

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 is the point.

2 ME. TANEJA: But the software project is  
3 an application. Okay? It is an application, so the  
4 application would be software, but it runs on these  
5 platforms.

6 ME. JUNG: Rest assured that single-  
7 failure criterion --

8 MEMBER BROWN: Single-failure criterion  
9 normally handles hardware.

10 ME. JUNG: -- has to be complied for  
11 systems.

12 MEMBER BROWN: It handles software. So I  
13 want you to understand that.

14 MEMBER ARMIJO: Would you repeat that?  
15 There were two conversations going on.

16 MEMBER BROWN: He says it's a software  
17 project; it runs on a platform, a computing platform.  
18 That's software. They're not doing a software  
19 failure, single-failure or FMEA or software analysis.  
20 That's not what they're doing, because they don't  
21 have it.

22 ME. SANTOS: But --

23 MEMBER BROWN: Hold it, Dan.

24 It's in a cabinet. It's in a system.  
25 They are analyzing that overall system effectively for

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *single-failure --*

2 *ME. TANEJA: Right, right.*

3 *MEMBER BROWN: And, oh, they've got this*  
4 *platform in it. That's all it is. It's a computing*  
5 *box, and everything else is hung off of it. That's*  
6 *what they're doing the single-failure criterion*  
7 *against.*

8 *ME. TANEJA: The IEEE 603 scope --*

9 *MEMBER BROWN: Can this be yes or no?*

10 *ME. TANEJA: No. It is -- no. Let me*  
11 *just lay out IEEE 603 scope starts at the sensor, goes*  
12 *all the way to execute level, right? The computation*  
13 *level is within the scope of the IEEE.*

14 *MEMBER BROWN: That's a box.*

15 *ME. TANEJA: So, when we look at the*  
16 *single failure, it is the entire from sensor to the*  
17 *execute when we look at a single failure, any failure*  
18 *within that division, whether it is a software failure*  
19 *or hardware failure. The safety function needs to be*  
20 *performed in the presence of a single failure.*

21 *Now, you know, there it is really very*  
22 *difficult to separate software and hardware. I mean*  
23 *they are integrated. So, when we look at a single*  
24 *failure --*

25 *MEMBER BROWN: We're getting wrapped*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 around this and we're confusing everybody.

2 ME. SANTOS: Let me clarify this. I  
3 understand what you're asking, Charlie.

4 Dan Santos from the staff.

5 As part of this software project -- and  
6 we're getting hung up on the terminology - an FMEA  
7 report will be developed. Okay? The FMEA will  
8 analyze the hardware --

9 MEMBER BROWN: Yes.

10 ME. SANTOS: -- for single-failure  
11 criteria. The hardware, Charlie.

12 MEMBER BROWN: Yes, but you look at  
13 evaluating a single failure from the design that is  
14 handed to you in the DCD. You look at that  
15 architecture --

16 ME. SANTOS: Correct.

17 MEMBER BROWN: -- and you evaluate that  
18 architecture for failures of parts that are  
19 illustrated in that design and how it is  
20 interconnected?

21 ME. SANTOS: Correct.

22 MEMBER BROWN: So, all I'm trying to do is  
23 make sure we have got the right calibration. You have  
24 enveloped the whole hardware/software integrated  
25 package as a software project?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   ME. SANTOS: Correct.

2                   MEMBER BROWN: But it's not --

3                   ME. TANEJA: Well, you know, we basically  
4 look at that system level.

5                   ME. SANTOS: That's correct.

6                   MEMBER BROWN: If you really want to get  
7 out of this hole, you ought to stop, Dan.

8                   ME. SANTOS: We need to move on.

9                   MEMBER BROWN: We ought to move on,  
10 please.

11                   ME. SANTOS: Yes.

12                   MEMBER BROWN: Is that okay, Mr. Chairman?

13                   ME. SANTOS: We got hung up on the  
14 terminology.

15                   ME. TANEJA: All right. There is the DAC  
16 that is in table 2.2.15 on criteria 5.1. The action  
17 here is that the inspection of these software  
18 projects, design phase summary BRR, shows that an FMEA  
19 has been completed. Okay?

20                   Now the acceptance criteria, if you look  
21 at it, it is basically restating the IEEE 603  
22 definition of a single failure, which says that the  
23 FMEA has been completed and shows that the software  
24 projects safety-related functions required for design  
25 basis events can be performed in the presence of all

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 those three criterias of the single-failure  
2 definition, as defined in 603.

3 ME. JUNG: This is the example that we are  
4 going to drill down to provide you some information,  
5 how we got to this DAC and how we came to a conclusion  
6 on compliance with the regulation as part of the  
7 licensing basis.

8 ME. TANEJA: Okay. Now, you know, in the  
9 previous slide, I referred to this --

10 MEMBER BROWN: What is the BRR again?

11 ME. TANEJA: That is what I was going to  
12 get into.

13 MEMBER BROWN: Well, what is it?

14 ME. TANEJA: It's a Baseline Review  
15 Record, like the slide title states.

16 MEMBER BROWN: Is that the slide title?

17 ME. TANEJA: Oh, on the next slide.

18 MEMBER BROWN: Thank you. Thank you. I  
19 was still on page 69, and I hadn't turned the page  
20 yet.

21 CHAIRMAN BLEY: Please go ahead.

22 ME. TANEJA: Well, I knew that was going  
23 to come up. That is why we put that slide in there.

24 The Baseline Review Record for the ESBWR  
25 design, as described in Tier 1, Section 3.2, you know,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 a BRR will be prepared at the conclusion of each  
2 software life cycle phase for each of the seven  
3 software projects.

4 So we will have a BRR summary report at  
5 the planning phase, requirements phase, design phase,  
6 implementation phase, and so on, for each of the seven  
7 software projects.

8 MEMBER ARMIJO: So far, there is no BRR?

9 ME. TANEJA: So far, there is no BRR. It  
10 is a DCD. We have not gotten into any implementation  
11 yet. But that is what the DAC laid out.

12 MEMBER ARMIJO: I understand. I just  
13 wanted to know if something had already been prepared  
14 at some phase.

15 ME. TANEJA: Right. And the DACs that are  
16 in Section 2.2.1.5, the BRR will be prepared at the  
17 conclusion of the design phase that demonstrates  
18 compliance to each IEEE 603 criteria.

19 Next slide, please.

20 CHAIRMAN BLEY: We don't have any of these  
21 yet, right, from anybody? The two slides together  
22 leave me a little vague. One says we document  
23 compliance, which could just say we have done it, and  
24 the other one says demonstrate compliance, which  
25 implies that it really is a thorough analysis within

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 the BRR. The BRR is to be an analysis that you can  
2 review.

3 Go ahead.

4 ME. TANEJA: You know, we have the two  
5 technical reports, the Tier 2\* reports --

6 CHAIRMAN BLEY: Yes.

7 ME. TANEJA: -- that we received from GEH.  
8 Those describe the format of the BRR and the contents  
9 of the BRR, what they would have. Okay?

10 MEMBER ARMIJO: Let me ask my question  
11 another way.

12 ME. TANEJA: Yes.

13 MEMBER ARMIJO: The AP1000 is further  
14 along in these various phases.

15 ME. TANEJA: Right.

16 MEMBER ARMIJO: Do you have BRRs? Do they  
17 exist for the AP1000? So we could at least look at  
18 them?

19 ME. JUNG: Not that we know of.

20 ME. SANTOS: They are not called that.

21 ME. JACKSON: The AP1000 design, they  
22 don't follow this exact process that GEH developed.  
23 They don't have Baseline Review Records.

24 MEMBER ARMIJO: Because they are closing  
25 it out in the amendment, I guess?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           ME. JACKSON:     But they do have other  
2 reports that summarize the activities, such as like  
3 V&V summary reports.

4           MEMBER ARMIJO:   Okay.

5           ME. JACKSON:     Safety analysis reports.

6           MEMBER ARMIJO:   Well, it doesn't exist --

7           ME. JUNG:        To the staff, what it meant is  
8 these BRRs would be a medium between -- these are full  
9 of documentation during the inspection stage. Rather  
10 than staff trying to dig it through, BRR will  
11 summarize.     Under their 2A program, they will  
12 summarize what they have done to complete their  
13 activities for their particular software project for  
14 that life cycle phase.

15                   Staff will look at that, and staff will  
16 also have a point, "Oh, okay, you said you did all  
17 this." We'll go into these individual reports, read  
18 the individual lines, and say, "Yes, we agree with  
19 you.     This life cycle you guys completed is  
20 acceptable."     That's the staff's determination of  
21 adequate resolution of that particular activity.

22           ME. SANTOS:     This is Dan Santos from the  
23 staff.

24                   From a technical standpoint, different  
25 vendors will have different terminologies, but our

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 guidance is the same in terms of the life cycle and  
2 BTP 714. So, whether GE might be BRR and Westinghouse  
3 could be a collection of documents, the scope that the  
4 staff will look at and the level of depth is  
5 equivalent. So, they might map differently, but at  
6 the end of the day the collection is the same level of  
7 rigor for the life cycle development process.

8 MEMBER BROWN: When does a BRR get  
9 developed?

10 ME. TANEJA: At the conclusion of each  
11 life cycle phase.

12 MEMBER BROWN: Is that after COL?

13 ME. TANEJA: Like --

14 MEMBER BROWN: Is that after COL?

15 ME. SANTOS: Yes, the expectation --

16 ME. TANEJA: Well, like Laura explained,  
17 three different ways of closing out --

18 MEMBER BROWN: I know there's different  
19 ways. Just let's pick one. Somebody is going to --

20 ME. TANEJA: The expectation --

21 ME. SANTOS: It's up to -- it's not my --

22 MEMBER BROWN: No, no. I mean pick one.

23 MS. DUDES: Guys, guys. Charlie, the  
24 answer is yes. For ESBWRs, the answer is yes.

25 MEMBER BROWN: It is post-COL?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   ME. TANEJA: Yes, sir.

2                   MEMBER BROWN: Yes. Thank you.

3                   ME. TANEJA: Okay. Yes.

4                   MEMBER BROWN: We are working on that.

5                   (Laughter.)

6                   ME. TANEJA: Yes. And similarly, I guess  
7 the Tier 1, this is a quote from Tier 1, 2.2.1.5. It  
8 states that, "The demonstration of compliance with  
9 IEEE 603 means the Q-DCIS documentation includes  
10 design bases that make appropriate reference to IEEE  
11 603 design criteria and that the resulting as-built  
12 equipment has been inspected, tested, or analyzed to  
13 show that the Q-DCIS will be capable of performing in  
14 accordance with the design bases."

15                   And the second bullet is also a quote from  
16 2.2.15, which basically talks to the method of doing  
17 the inspection or analysis or testing of a given  
18 requirement. And the examples would be the DAC  
19 2(b)(1) in 3.2 has a requirement phase. "Output are  
20 inspected and analyzed for RTIF software project."  
21 And DAC 3.2(1)(h)(1) states that, "The inspection of  
22 the software safety plan for the RTIF software project  
23 will be performed."

24                   So there is inspections. There is  
25 inspections and analysis, and there is either

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 inspection analysis and the test. So a lot of these  
2 activities are laid out within that column of the  
3 ITAACs.

4 Next slide, please.

5 And the Tier 2 DCD for ESBWR, the table  
6 7.1-2 in Tier 2 provides a roadmap to sections of the  
7 Tier 2 DCD. That documents the single-failure  
8 features for each of the plant process safety system.

9 The 19 plant process safety systems  
10 individually implement single-failure design features  
11 which are implemented on seven software projects that  
12 comply with the IEEE 603 Clause 5.1. And these seven  
13 software projects are implemented on three platforms  
14 that are also single-failure proof.

15 And my point was the single-failure proof  
16 is system, software project, and hardware. It is  
17 basically everywhere. Okay?

18 Next slide, please.

19 And this table 7.1-1 in Tier 2, all 19  
20 plant process safety systems implement on three  
21 diverse platforms using the same software projects,  
22 comply with single-failure design-related regulations.

23 That is 50.55a(a)(1), 50.55a(h), GDC 21, and GDC 23.

24 Next slide.

25 Similarly, all of the safety systems

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 within Q-DCIS conform to Reg Guide 153 that provides  
2 guidance on application of single-failure criteria to  
3 safety systems.

4 Compliance to IEEE 603 criteria are  
5 documented in Tier 2, Section 7.1.6.6.1.2 and Section  
6 7.1.6.6.1.1. So, the 7.2, 7.3, they talk specifically  
7 to the systems, and then 7.1, Tier 2, talks  
8 specifically compliance to the IEEE 603 criterias.

9 The 7.1.6.6.1.1 states that criterion 4.1  
10 requires identification of equipment protective  
11 provisions that prevent the safety system from  
12 accomplishing their safety function. Safety-related  
13 systems are designed to accomplish safety-related  
14 functions in accordance with the single-failure  
15 criteria of 603, 5.1. The FMEA confirms the detailed  
16 design implementation of the safety-related systems to  
17 a single-failure criteria, as described in the DCD.

18 So, these clauses of 603 are very well  
19 laid out in Section 7.1 of the Tier 2 DCD.

20 Next slide, please.

21 CHAIRMAN BLEY: The tables you just ran  
22 through, the matrices --

23 ME. TANEJA: Right.

24 CHAIRMAN BLEY: -- the purpose of this  
25 exercise is to show us that, in fact, the reviewer or

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the inspector is provided with links back to specific  
2 sections in the DCD and specific regulations to guide  
3 their inspection or their review, depending on  
4 which --

5 ME. TANEJA: Right. The way this thing is  
6 structured for ESBWR, it makes it very easy for even  
7 the reviewer and the inspectors to really follow this  
8 roadmap to verify compliance with these different  
9 regulations.

10 CHAIRMAN BLEY: So, at this level, some of  
11 the things Charlie was asking about before in  
12 AP1000 --

13 ME. TANEJA: Right.

14 CHAIRMAN BLEY: -- you would claim you  
15 have identified here?

16 ME. SANTOS: Correct.

17 ME. TANEJA: You know, like for this  
18 table, I mean I have section numbers that I can go  
19 through here for each of the safety systems.

20 CHAIRMAN BLEY: These are the DCD section  
21 numbers?

22 ME. TANEJA: Yes, DCD section numbers,  
23 right. I mean I just gave an example of the 5.1  
24 Clause. I mean this table covers all the clauses.

25 CHAIRMAN BLEY: Now the AP1000 folks

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 didn't show us anything like this. Does something  
2 like this exist for all the Design Centers or is this  
3 just the ESBWR?

4 ME. TANEJA: I guess we are learning.

5 (Laughter.)

6 ME. JUNG: There is no regulation that  
7 they have to have this.

8 CHAIRMAN BLEY: But I worry, how is an  
9 inspection procedure going to be written or how is an  
10 inspector or a reviewer going to find the right places  
11 and the right information? It looks like you have  
12 catalogued here, but none of the other projects have  
13 done that.

14 ME. SANTOS: This is Dan Santos.

15 CHAIRMAN BLEY: So we still have to do  
16 that somehow.

17 ME. SANTOS: Yes. The same people  
18 involved with the review of those DCDs are the same  
19 ones that are going to be heavily involved with the  
20 development on the inspection procedures, and we are  
21 going to hear that later today.

22 CHAIRMAN BLEY: Okay.

23 ME. TANEJA: We have done mapping.

24 CHAIRMAN BLEY: You gave me a nice flag  
25 because I wanted to say this before Tom had to stand

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 up and tell us what was going on.

2 The way you just said that makes me  
3 wonder, will there be an inspection procedure for  
4 every ITAAC or will there be general inspection  
5 procedures? And, if so, that means the only way to  
6 really have comfort in this stuff all being picked up  
7 is that the people who did the reviews are heavily  
8 involved, but some of them the reviews are kind of  
9 old, and probably nobody has this in their head  
10 anymore. And it just strikes me as a heck of a job  
11 they are going to have to do.

12 MS. DUDES: Oh, no, I don't think we  
13 underestimate the level of rigor that we would  
14 approach under inspection associated with I&C. I have  
15 written down and shared, and we have talked about the  
16 concern in terms of the specificity in the ITAAC and  
17 DAC, and then how it relates back to the design  
18 document.

19 And I think Tom will talk a little bit to  
20 the approach of how you develop an inspection  
21 procedure, how an inspection is conducted overall. I  
22 mean, even in the current environment with the  
23 operating reactors, there is the final safety analysis  
24 report, but an inspector does not stop there in  
25 preparing for, developing their inspection plans and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *procedures, delving into design bases and other*  
2 *reports.*

3 *So, hopefully, we will be able to share*  
4 *with you our approach to how we are going to make sure*  
5 *that we do address the critical aspects. And*  
6 *fundamentally, in an ITAAC closure, for example, I*  
7 *mean we have to step back and remember that we expect*  
8 *the licensees at that time, they own and are*  
9 *responsible for closing those ITAACs, submitting under*  
10 *oath or affirmation to us that they have done that,*  
11 *and meeting their license.*

12 *That being said, we will, of course,*  
13 *conduct the same types of rigorous inspections that we*  
14 *conduct today in the field and, then, obviously,*  
15 *during construction, to assure that we are addressing*  
16 *that.*

17 *And when we inspect, in particular, things*  
18 *that are a little bit more detailed design*  
19 *inspections, there is a level of rigor associated with*  
20 *delving into what the established licensing basis is,*  
21 *getting appropriate guidance and documents, and*  
22 *developing those procedures.*

23 *And I am almost giving part of Tom's*  
24 *presentation.*

25 *ME. FREDETTE: Take it away.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (Laughter.)

2 MS. DUDES: So I think we'll move on with  
3 that.

4 But I think what these first two  
5 presentations are really trying to focus us on is the  
6 level of rigor, depth, and detail that the staff goes  
7 to, to establish the licensing basis and make the  
8 safety finding upfront.

9 The regulatory imprint on safety does not  
10 stop here. Then it goes to, then, the level of rigor  
11 that the staff approaches to their inspection  
12 procedures.

13 And I know we have heard a lot about the  
14 wording, but, as they walk through, they are  
15 demonstrating that this detail and these critical  
16 elements do exist within the licensing basis. They  
17 are in the DCD. They are in the Tier 2 information.

18 We are hearing the challenge, and I have  
19 captured that, that maybe the roadmap is not so clear  
20 for some of the vendors, and it is a tougher challenge  
21 for a regulator to tell people how to format. And  
22 what you get to see here is that in the ESBWR that  
23 they really did insist on, and they are working  
24 through, maybe a clearer roadmap.

25 So I know I didn't actually fully answer

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that concern, but we are going to keep coming back to  
2 that because I think we have talked about that several  
3 times in terms of what is contained in the licensing  
4 basis and how can we assure ourselves that we are  
5 actually verifying that licensing basis at the  
6 inspection stage.

7 **MEMBER ABDEL-KHALIK:** Let me just repeat  
8 that point. You know, you are showing a lot of  
9 documents, and the point has been made many times that  
10 the safety case is made on the basis of a great deal  
11 of information in the DCD as well as many other  
12 documents, whether they are licensing topical reports,  
13 technical reports, et cetera.

14 And the question is, for those DAC that  
15 would be approved beyond the COL stage through an  
16 inspection process, can you, indeed, write a general  
17 inspection procedure that would allow the inspector to  
18 touch all those pieces of information on which the  
19 safety case was made?

20 **MS. DUDES:** In short, I am going to say,  
21 yes, we believe the answer is yes.

22 **MEMBER ABDEL-KHALIK:** You can write the  
23 general procedure applicable to all DAC that would  
24 allow the inspector to identify and touch all the  
25 relevant information in all these different sources on

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1       *which the safety case was made?*

2                   *MS. DUDES: Yes.*

3                   *MEMBER ABDEL-KHALIK: Okay. We will, I*  
4       *guess, have to wait to see.*

5                   *MS. DUDES: Okay.*

6                   *MEMBER ABDEL-KHALIK: Thank you.*

7                   *MEMBER ARMIJO: Just to follow up a little*  
8       *bit on that for an example, in your page 69 slide, the*  
9       *BRR acceptance criteria is that an FMEA has been*  
10      *completed and demonstrates a number of things. Now*  
11      *will your inspector or inspectors dig into that FMEA*  
12      *to see that it is adequate? You know, the quality of*  
13      *that FMEA, the people who did it, and how thoroughly*  
14      *it's done. Or will it be something else?*

15                   *Because, that way, you can say, okay, the*  
16      *tool, the FMEA was done well enough to reach the*  
17      *conclusion in the BRR that we don't have a single-*  
18      *failure issue. And that's really where I keep coming*  
19      *back is, at which point does the process turn into a*  
20      *design review? And you may want to call it an*  
21      *inspection. I don't care what you call it. But what*  
22      *I'm looking for is a design review.*

23                   *ME. SANTOS: And you are correct, it will*  
24      *be the former, the level and rigor. We actually have*  
25      *slides coming up on that, but when we get to those*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 slides, let's touch on that and actually what the  
2 expectations are, not from a process standpoint, from  
3 an I&C. You know, I opened this book that has all  
4 these tables. What is it that I am actually looking  
5 at?

6 So let's get to that slide and let's try  
7 to demonstrate. But, again, that would be the  
8 expectation because they haven't created it, but I  
9 think it is a pretty good explanation of what we will  
10 expect to see regarding that FMEA and the level of  
11 rigor we expect.

12 MEMBER ARMIJO: Okay. Thank you.

13 ME. SANTOS: So we will come back to that.

14 ME. TANEJA: The other thing that we found  
15 when we were reviewing this thing, that the single-  
16 failure criteria is integrated in the overall Q-DCIS.  
17 Redundancy and independence is implemented at the  
18 division level, at system level, and at the logic  
19 level, where appropriate.

20 In the next few slides, I will go over the  
21 examples of these single-failure design features  
22 implemented at these various levels.

23 Like we heard, the next slide, this is the  
24 example of a division-level single failure. In this  
25 design, the intradivisional and safety to non-safety-

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 related fiberoptic cable communication paths are  
2 redundant. That supports reliability and diagnostic  
3 capability.

4 So, here, you know, again, we don't lose  
5 any functionality under a single-failure scenario. No  
6 single failure of any single hardware component in any  
7 one division can lead to an inadvertent trip.

8 The safety-related cabinets and chassis  
9 are powered by redundant safety-related UPS.

10 And for the interdivision communication,  
11 no single failure or communication line or power  
12 failure results in loss of safety function.

13 This conforms to the ESBWR N-2 design  
14 philosophy. That is, one division can be out of  
15 service; the remaining three divisions can perform the  
16 safety function in the presence of a single failure.

17 Next slide, please.

18 MEMBER BROWN: That is what is meant by  
19 the "2"? N-2 is you can have a division out and you  
20 can have a single failure in any other division?

21 ME. TANEJA: Right. That's what the  
22 N-2 --

23 MEMBER BROWN: Clarified what N-2 means.

24 ME. TANEJA: All right, next slide.

25 Now this is the example of a system-level

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 implementation. We used the example of reactor  
2 protection system. The RPS is implemented on the  
3 RTIF/NMS platform using the RTIF software project.  
4 And the RPS is organized in four physically- and  
5 electrically-isolated divisions which utilize the  
6 principle of independence and redundancy for single-  
7 failure criteria as defined by --

8 MEMBER BROWN: One comment, Dinesh.

9 ME. TANEJA: Yes.

10 MEMBER BROWN: Recognize in that first  
11 bullet where it says "four physically-and  
12 electrically-isolated", electrically-isolated does not  
13 mean independence in these designs.

14 ME. TANEJA: Right.

15 MEMBER BROWN: It's just electrically-  
16 isolated?

17 ME. TANEJA: Isolated, right.

18 MEMBER BROWN: I just wanted to clarify  
19 that because that's not the way it used to be for the  
20 most part.

21 ME. TANEJA: Yes. Yes. Yes, we are  
22 basically focusing on the single failure right now.

23 MEMBER BROWN: Yes, I understand that.

24 ME. TANEJA: Right.

25 MEMBER BROWN: I stopped you; I just

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 wanted to make people understood the terminology.  
2 That's all.

3 ME. TANEJA: Yes, but I agree with you.

4 MEMBER BROWN: There's nothing else you  
5 can go on?

6 ME. TANEJA: Yes. So, the RPS system  
7 design also complies with the N-2 requirements, and  
8 the analysis complying with IEEE 379 will be used to  
9 confirm the safety-related system design conformance  
10 to the single-failure design.

11 And this graphically shows the RPS system  
12 and the redundancies of the four divisions, which it  
13 is really just a graphic representation.

14 MEMBER BROWN: It just represents the  
15 fuzzy independence --

16 (Laughter.)

17 CHAIRMAN BLEY: Too bad.

18 MEMBER BROWN: You have got to have a  
19 little humor in here somewhere, troops.

20 ME. TANEJA: At the logic level, ADS  
21 logic-level example, each division of SSLC/ESF is  
22 configured such that all functions are implemented in  
23 the PMR processors to support the requirement that a  
24 single divisional failure cannot result in advertently  
25 opening the ADS valve.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           Okay. It is not possible to lose a  
2 *single-failure inadvertent actuation protection by any*  
3 *operator or disable/test switch action. No single*  
4 *failure of sense, command, or execute features that*  
5 *includes sensors and the actuators can prevent the*  
6 *successful system operation as long as any three or*  
7 *four divisions of the safety-related power are*  
8 *available.*

9           Next slide, please.

10           In this slide, we are looking at the  
11 *example of single failure. What I wanted to provide,*  
12 *like this graphic depicts a number of overlapping*  
13 *inspection, testing, or analysis opportunities to*  
14 *verify compliance with single-failure criteria.*

15           The system ITAAC, for example, like the  
16 *rod control and information system, Section 2.2.1,*  
17 *would have a system-level ITAAC. The IEEE 603*  
18 *compliance would be another DAC or an ITAAC at 2.2.15.*

19           Then, software development, we have at 3.2 there is  
20 *a software development DAC; we are looking at the same*  
21 *thing. There is a lot of overlapping inspections*  
22 *happening.*

23           You know, the Tier 1 summarizes the design  
24 *features that are contained in Tier 2, and Tier 2,*  
25 *7.1, gives the specific compliance, gives the design*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 information and it provides compliance to the  
2 regulation and standard and the guidance that are  
3 applicable to that, in this example like a single-  
4 failure criteria.

5 So I just wanted to show that each system,  
6 each platform, each logic, there is multiple  
7 opportunities of testing and inspections. They are  
8 very interrelated and they are overlapping. So we  
9 will have plenty of opportunities to be able to  
10 inspect and test these things.

11 MEMBER ARMIJO: I just want to ask a  
12 question.

13 ME. TANEJA: Yes.

14 MEMBER ARMIJO: Typically, the inspections  
15 are a sampling process.

16 ME. TANEJA: True.

17 MEMBER ARMIJO: Now, in this case, is it  
18 going to be extremely heavy sampling? Is it going to  
19 approach 100 percent? I am just trying to get a feel  
20 of how much of these DACs and ITAACs you are going to  
21 really dig into in the inspection process.

22 ME. SANTOS: Can we have the inspection  
23 folks answer the question?

24 MEMBER ARMIJO: And I will defer, as long  
25 as they address that.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   ME. SANTOS: Thank you.

2                   ME. TANEJA: The Tier 2, this slide is  
3 basically the compliance of the Q-DCIS for single-  
4 failure criteria as implemented and verified during  
5 the software life cycle development process, you know,  
6 all these phases.

7                   The IEEE 603 --

8                   MEMBER BROWN: Answer me one question  
9 relative to this.

10                  ME. TANEJA: Yes.

11                  MEMBER BROWN: You are talking about all  
12 your various opportunities.

13                  ME. TANEJA: Right.

14                  MEMBER BROWN: Let me ask the question  
15 correctly here. Are you reviewing their process? In  
16 other words, that they ran it, they did the single  
17 failure, and they provide a matrix that says there's  
18 no single failure?

19                         Or are you performing a sample design  
20 review of certain selected single failures that you  
21 may foresee, based on your looking at the overall  
22 architecture and an analysis independently that says,  
23 yes, they covered that and we validated or agree that  
24 that was covered?

25                         Do you understand my question?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           ME. TANEJA: Yes, I understand.

2           MEMBER BROWN: Is it all process, that  
3 they followed their process, generate it, they got a  
4 matrix that says we analyzed all these 274 failure  
5 modes or failure specifics, and you say, "Check, they  
6 did that."? Or do you take critical functions that  
7 you think are very important as opposed to some that  
8 are maybe of lesser importance because they result in  
9 some result, I mean some scram or whatever, but you  
10 take one that you know is critical to the performance,  
11 and then you go look and you look at the actual  
12 design? Where is the actual design review executed as  
13 part of your DAC result review?

14           ME. SANTOS: The expectation is, once they  
15 actually have implemented --

16           MEMBER BROWN: When there is a design, a  
17 complete design, when they have hardware, wires --

18           ME. SANTOS: Correct.

19           MEMBER BROWN: -- schematics, all that  
20 kind of stuff.

21           ME. SANTOS: Remember, the FMEA, as part  
22 of the BRR -- hold on. It's going to keep evolving,  
23 okay, through the life cycles. So the expectation is  
24 to actually grab the FMEA, the actual report, open it  
25 up, not only assess the quality of it, that it is a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 good FMEA, but then drill down. Do they have the  
2 credible failure modes in there? Does the level of  
3 abstraction match to the architectural drawing, and  
4 does it flow from the high-level architecture all the  
5 way to the replacement module level? And does it  
6 identify failure modes, mitigations? Everything maps  
7 together? That is the level of rigor our expectation  
8 is in the inspection process that we are going to go  
9 through.

10 MEMBER BROWN: And that will be done by  
11 whom?

12 ME. SANTOS: That will be done by the  
13 team, the inspection team, which includes --

14 MEMBER BROWN: Okay. I'm with you.

15 ME. SANTOS: -- agency experts.

16 MEMBER BROWN: Okay.

17 ME. SANTOS: That includes the correct  
18 agency expert with the right level of knowledge for  
19 the task at hand. So, in this case, it will be folks  
20 like Dinesh accompanied by folks from the region,  
21 accompanied by other support they might need on the  
22 inspection team. So, Dinesh will be opening that FMEA  
23 with others and going through it.

24 MEMBER BROWN: Does your all's review  
25 process document that approach or is it --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           CHAIRMAN BLEY:   Charlie, I think we will  
2 wait for Tom.

3           MEMBER BROWN:   Okay. Well, no, Tom is in  
4 the region.

5           ME. SANTOS:   No, Tom is here.

6           CHAIRMAN BLEY:   Tom is here.

7           MEMBER BROWN:   Is he here?

8           ME. SANTOS:   Yes.

9           MEMBER BROWN:   Oh, he's here? Okay.

10          CHAIRMAN BLEY:   He is here.

11          MEMBER BROWN:   All right.

12          CHAIRMAN BLEY:   He is leading this  
13 development of the --

14          ME. SANTOS:   We are getting there, but,  
15 technically, we are diving into the actual report.

16          ME. JUNG:   Tom's current job is in DCIOP.  
17 Prior to that, he used to work for me as an engineer  
18 for some time.

19          MEMBER BROWN:   Okay.

20          ME. SANTOS:   And let me give you an  
21 example from AP1000. They actually are on Rev 2, like  
22 three Revs of their --

23          MEMBER BROWN:   Go ahead and get finished.

24          ME. TANEJA:   Okay. The single-failure  
25 criteria is present throughout the software life

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 cycle, software project life cycle process. Each  
2 safety system implements the life cycle process. And  
3 the DAC and the ITAACs are resolved and completed  
4 during the implementation of these software life  
5 cycles.

6 For the ESBWR design, we have two  
7 licensing topical reports as Tier 2\*, and these two  
8 documents, the software manual, the program manual,  
9 and the software QA assurance manual, these documents,  
10 you know, we reviewed them. These form the basis for  
11 developing the planning documents for each of the  
12 software projects.

13 So these provide the criterias, and then  
14 the DACs are there in 3.2 for each of the planning  
15 phases for each of the software projects which need to  
16 conform to the criterias that are laid in here. And  
17 these get pretty specific. I mean they lay out all  
18 the phases of the software life cycle, and they also  
19 lay out the deliverables at each phase. We reviewed  
20 them and we found them to be acceptable.

21 ME. JUNG: Charlie, earlier you asked  
22 about the life cycle development, where is the certain  
23 performance criteria for certain elements of the  
24 design development. I think these two topical  
25 reports, licensing topical reports, actually contain

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *some of the critical performance criteria expected to*  
2 *be observed and verified.*

3 *MEMBER BROWN: Yes, but that's on the*  
4 *software you are developing. I mean that's what they*  
5 *are. That is software --*

6 *ME. JUNG: By the time you get to*  
7 *integration with the hardware, you know, you cannot --*

8 *MEMBER BROWN: I understand that. I*  
9 *understand that. You've got to integrate it, but it*  
10 *is a software --*

11 *ME. JUNG: Right.*

12 *MEMBER BROWN: It is a software*  
13 *development process.*

14 *ME. JUNG: Right.*

15 *MEMBER BROWN: I am not arguing about that*  
16 *-- yet.*

17 *ME. TANEJA: And I think Ian has already*  
18 *kind of referred to these things, you know, the amount*  
19 *of information that we reviewed.*

20 *In conclusion, staff found the I&C design*  
21 *in the DCD to have met the requirements of the single-*  
22 *failure criteria.*

23 *The next slide.*

24 *The DAC, you know, they provide for a*  
25 *thorough implementation of the single-failure criteria*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 throughout the life cycle process for each of the  
2 safety systems.

3 The Item 8a, acceptance criteria, you  
4 know, I pointed that out. That was the example that  
5 we put up of the DAC 8a. The BRR summarizes the  
6 detailed implementation of design. See, these were  
7 like some of the contents that are provided in GE's  
8 topical report as to the content of the BRR.

9 So, a Configuration Management Report, for  
10 example, Software Safety Analysis, the V&V Report, and  
11 secure development and operational environment, these  
12 are some of these subjects that are part of that BRR  
13 summary report. These are laid out in those topical  
14 reports as to the content of the BRR.

15 Next slide, please.

16 The staff found the I&C DAC to be adequate  
17 for verifying that the as-built I&C systems conform to  
18 the single-failure requirements described in the DCD.

19 And also, I will point out that on the  
20 last bullet, there is a COL information item in this  
21 design that requires the applicant or the licensee to  
22 notify the NRC at least six months prior to the  
23 scheduled completion of each BRR and software plan  
24 that is designated as DAC.

25 For each of those DAC-designated ITAACs,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the COL applicant is going to let us know six months  
2 prior to their completion. It gives us the  
3 opportunity to prepare for those inspections.

4 So, in conclusion, staff found the I&C  
5 design of the ESBWR to have met the requirements of  
6 single-failure criteria.

7 CHAIRMAN BLEY: Condition on the  
8 inspections?

9 ME. TANEJA: And with that, I am open up  
10 to -- hum?

11 ME. SANTOS: No, no.

12 CHAIRMAN BLEY: Not conditional on the  
13 inspections?

14 ME. SANTOS: No. We are going to get to  
15 that.

16 I want to make two points once Dinesh --

17 CHAIRMAN BLEY: Okay. Well, just before  
18 you do --

19 ME. SANTOS: Yes, sir.

20 CHAIRMAN BLEY: -- we don't have an  
21 implementation. We don't have the BRR. We have DAC.  
22 Make your point. I don't get how you get here  
23 without having those in place.

24 ME. SANTOS: Okay. When the staff  
25 presents their SER, the staff is concluding that the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 information contained in the applicant's DCD is  
2 necessary and sufficient to reach a safety finding.  
3 The additional information that gets generated by  
4 closing DACs or ITAACs helps gain a better  
5 understanding of the implementation of that safe  
6 design, but it will not alter the safety conclusion  
7 itself.

8 CHAIRMAN BLEY: As long as it satisfactory  
9 completes?

10 MS. DUDES: Well, I would say, as long as  
11 it meets the license.

12 CHAIRMAN BLEY: Right.

13 MS. DUDES: So we establish the licensing  
14 basis in our review.

15 ME. SANTOS: Right.

16 MS. DUDES: The safety finding establishes  
17 what licenses are required by law to meet at all  
18 times -- at all times -- those functions,  
19 descriptions, every single item.

20 I do understand the point about  
21 implementation. And a simple example is the DCD  
22 references a lot of pumps in it as well, but we don't  
23 actually know that that pump will deliver 350 GPMs  
24 until --

25 CHAIRMAN BLEY: Until you test it.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. DUDES: -- it is in the plant and  
2 operating, and there's an ITAAC to verify it.

3 And I promised I wouldn't go too much into  
4 process. But, I mean, part of this licensing process  
5 that we are in says you make your safety finding based  
6 on the descriptions in the DCD. And then, the nuance  
7 of ITAAC, which is a little bit different in this  
8 process, verifies the as-built condition. So we  
9 verify that the pump actually does put out 350 GPMs.  
10 The whole implementation part of the life cycle is  
11 verified through the ITAAC.

12 ME. SANTOS: So, when we come with that  
13 SER, that is the time to have the technical  
14 discussions with the oversight you provide to say and  
15 have the discussion: is there enough appropriate  
16 level of detail contained in the DCD to properly bound  
17 that we, indeed, have a safe design?

18 A quick example, Charlie, like in the old  
19 times, if I tell you I have a completely independent,  
20 or your definition, four-channel separate system, you  
21 don't necessarily need to know whether I use a  
22 TELEPERM or a Common Q, or whatever, platform to  
23 conclude that architecture provides features that will  
24 make it safe and meet our regulations.

25 If, on the other hand, you have a more

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 complex system with interconnectivity and fuzzy  
2 independence, it is appropriate to bring more detail  
3 in the DCD and not necessarily leave it to follow-on  
4 inspection activities.

5 So, the moment is now to make sure  
6 collectively the DCD has the correct level of detail  
7 to support the safety findings. And that is one point  
8 I wanted to make.

9 The other point is, going back to your  
10 question regarding the FMEA, not only do we use  
11 operating experience, LERs, international agreements,  
12 we also look at FMEAs that have recently been  
13 completed. Like the AP1000, I said it had gone  
14 through three revisions, improving the quality of that  
15 document. There is industry guidance like IEEE 352,  
16 359, or Reg Guides, and the expertise of the actual  
17 reviewer that will look at the key attributes in the  
18 FMEA, postulate credible failure modes, trace back to  
19 the architectural drawings contained in the license,  
20 and making sure everything flows all the way down to  
21 that module that was appropriately modeled as part of  
22 the FMEA.

23 So that is the level of rigor we expect.  
24 Whether it is an inspection or an audit, it is an  
25 equivalent level of technical rigor.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1                    *MEMBER ABDEL-KHALIK: Let me go back to*  
2 *the statement --*

3                    *ME. SANTOS: Yes, sir.*

4                    *MEMBER ABDEL-KHALIK: -- that you just*  
5 *made.*

6                    *Okay. I think you emphasized the fact*  
7 *that the safety case can be made, and is being made,*  
8 *based not only on the DAC, but on the information*  
9 *contained in the DCD and many other documents, as we*  
10 *discussed before. So what, in your view, is the*  
11 *purpose of the inspection?*

12                    *ME. SANTOS: To verify that the*  
13 *implementation by the applicant conforms to their*  
14 *licensing or design basis.*

15                    *MEMBER ABDEL-KHALIK: And that*  
16 *determination requires what?*

17                    *ME. SANTOS: The owner is the applicant,*  
18 *and it will require the NRC will have, as part of*  
19 *their inspection process, the right level of expertise*  
20 *to make sure they understand what is being presented*  
21 *in front of them. And I agree with that, confirm that*  
22 *verification.*

23                    *MEMBER ABDEL-KHALIK: I guess the question*  
24 *that we still have is whether or not that inspection*  
25 *process will, in fact, assure compliance with all the*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 requirements on which you have made the safety case.  
2 That is the heart of the argument.

3 ME. SANTOS: Thank you. I understand your  
4 point fully.

5 MEMBER ABDEL-KHALIK: Okay.

6 MEMBER ARMIJO: In the case of the FMEA,  
7 you mentioned for the AP1000 there's been three  
8 iterations --

9 ME. SANTOS: Uh-hum.

10 MEMBER ARMIJO: -- as it has been either  
11 reviewed by the staff or by the applicant. In the  
12 case of, let's say, ESBWR, if there is a problem with  
13 the FMEA, deficiencies in the FMEA or any of the other  
14 BRRs that you review or inspect, what happens then?

15 ME. SANTOS: Okay. Since it is going to  
16 be under inspection, that will generate -- if it  
17 cannot be resolved as part of the inspection itself,  
18 because there's some deficiencies that you do that, it  
19 will be a determination made whether it elevates to an  
20 actual inspection finding.

21 But this is outside my realm. I really  
22 would like for the inspection representative to fully  
23 answer that question.

24 MEMBER ARMIJO: Okay. And then, just one  
25 last one that may be in your scope is: how many

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 inspections do you contemplate for, let's say, ESBWR,  
2 the DAC for the ESBWR?

3 ME. TANEJA: Seven software projects.

4 MEMBER ARMIJO: Seven?

5 ME. TANEJA: Seven software projects,  
6 right?

7 MEMBER ARMIJO: Several different phases?

8 ME. TANEJA: All in phases. At the  
9 conclusion of each phase --

10 MEMBER ARMIJO: Do you have a number  
11 concluded?

12 ME. SANTOS: Yes. We have 100.

13 MEMBER ARMIJO: Okay. That is what I was  
14 looking for.

15 ME. TANEJA: The key is the scope. So  
16 numbers can be a little bit misleading. Okay?

17 MEMBER ARMIJO: I understand, but that is  
18 a lot of inspections.

19 ME. SANTOS: Right. For ESBWR, it will be  
20 hundreds.

21 ME. JUNG: My expectation is the agency  
22 must do the sufficient level of inspection to confirm  
23 that implementation of the design should be consistent  
24 with what is in the licensing basis to which the  
25 agency staff made a safety finding.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                    *MEMBER ARMIJO: Right. There's hundreds*  
2 *of inspections possible, but you do a sampling. And*  
3 *that gets back to my other question.*

4                    *ME. SANTOS: For the DACs, it will be 100*  
5 *percent of the hundreds for ESBWR.*

6                    *MEMBER ARMIJO: Okay.*

7                    *CHAIRMAN BLEY: Ready to go on to the*  
8 *next?*

9                    *MS. DUDES: Okay. Yes, I had some closing*  
10 *remarks, but I think we touched upon them because it*  
11 *was all about these first two presentations. I really*  
12 *appreciate the Committee the past several hours*  
13 *sitting through the details of this small slice, but I*  
14 *think the staff appreciated the opportunity. We*  
15 *weren't trying to re-review these designs as much as*  
16 *demonstrate that the safety finding -- we really are*  
17 *confident, when we are submitting our SER to the*  
18 *Commission for rulemaking, that we have established a*  
19 *safety basis in the DCD, and that we are confident*  
20 *that the agency will be able to inspect that and*  
21 *verify the as-built configuration of these plants.*

22                    *So, I am not going to belabor that. I*  
23 *think we have made that point.*

24                    *CHAIRMAN BLEY: Yes.*

25                    *MS. DUDES: I think we have discussed it.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           But I appreciate -- I know you have sat  
2 through a lot of technical presentations, and this was  
3 really just trying to demonstrate our confidence in  
4 our safety findings.

5           So, now Tom seems to be the man of the  
6 hour because there's been a lot of questions that have  
7 been redirected over to him. So I would ask Tom  
8 Fredette -- I don't know if you wanted to keep going  
9 or --

10           CHAIRMAN BLEY: Yes.

11           MS. DUDES: Okay.

12           CHAIRMAN BLEY: We just had a break,  
13 right?

14           MEMBER BROWN: While he is setting up, I  
15 would just like to make one observation from my  
16 perspective relative to the inspections, reviews,  
17 whatever.

18           It is the thoroughness and level of detail  
19 of those reviews that we have tossed back and forth  
20 several times. Is it going to approximate the level  
21 that we see during a design certification review where  
22 there is a very strong -- in those areas where you had  
23 what I call mushy block diagram-type designs? You  
24 know, when you are talking about pipes, you know, a  
25 pipe is a pipe. It's blacksmith technology.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           But the I&C world, the brains, the nerve  
2 center, it is not a support system. I have a little  
3 bit disagreement. But I would expect the time that  
4 was spent, you need to review that design as well as  
5 the DACs and ITAACs, but you can't just depend on  
6 those, once you see that final design. You have to  
7 see the design to make sure it is within the  
8 boundaries within which you made your determination  
9 that the DACs and the ITAACs kind of covered the  
10 waterfront because it may not be --

11           ME. SANTOS: I agree with that.

12           MEMBER BROWN: Any particular implements  
13 could be different, very different.

14           That is on the record. I just wanted to  
15 get that on the record. That is the point.

16           ME. FREDETTE: Good afternoon, everyone.

17           My name is Tom Fredette from the Division  
18 of Construction Inspection and Operational Programs,  
19 the Construction Inspection Programs Branch, in that  
20 Division.

21           Just by way of intro, we formed the DAC  
22 Task Working Group just about a year ago. I'm the  
23 lead for that group. So, procedures, process,  
24 inspections of DAC are all coordinated and developed  
25 by my group.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           I have come here today, as a follow-on to  
2 Ian and Dinesh and Kimberly's presentation, I wanted  
3 to just give the Committee an overview of our DAC  
4 inspection approach. And as a follow-on to the  
5 example that you used for single-failure criterion, I  
6 am going to go through briefly how we apply inspection  
7 guidance to that particular example.

8           Next slide.

9           First and foremost, I just want to get  
10 fundamentally -- and this has been mentioned several  
11 times already -- as with all DAC inspection, it is a  
12 verification that the design, the safe design that has  
13 been determined to be safe as implemented will conform  
14 to the licensing basis. That is our fundamental  
15 objective.

16           Since DAC are all ITAAC, DAC inspection is  
17 fundamentally an ITAAC inspection and is subject to  
18 the rules of ITAAC inspection for Part 52. DAC  
19 inspection is independent of the licensing decision.

20           Now that is just a point to make here. We  
21 talk about the licensing decision that has already  
22 been made, but, as with all ITAAC, they are there to  
23 support verification that the facility will conform to  
24 the licensing basis, and that when the ITAAC are  
25 complete, the results will support a later Commission

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 *finding per 103G that the facility is safe to load*  
2 *fuel and operate.*

3 *DAC inspection has no impact on the safety*  
4 *finding. Regardless of what we find in inspection*  
5 *space, the safety finding does not change. DAC*  
6 *inspection is not an indication that the ITAAC is*  
7 *complete.*

8 *MEMBER BROWN: Can you explain that to the*  
9 *uninitiated, though? I mean, if you find, for*  
10 *instance, in the review of the I&C system that it is,*  
11 *in fact, not independent, just hypothetically it is*  
12 *not independent --*

13 *ME. FREDETTE: In other words, they have*  
14 *done something in implementation that has compromised*  
15 *the safe design?*

16 *MEMBER BROWN: Yes. Yes. So, why doesn't*  
17 *that have an effect on the safety finding? I*  
18 *understand it is independent of the licensing*  
19 *decision.*

20 *ME. FREDETTE: Yes.*

21 *MEMBER BROWN: That is a different issue.*

22 *ME. FREDETTE: That would be a poor*  
23 *implementation of the safety --*

24 *MEMBER BROWN: How about an unsatisfactory*  
25 *implementation?*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           ME. FREDETTE: Yes, unsatisfactory, yes.

2           MEMBER ABDEL-KHALIK: That would be  
3           communicated through a Notice of Violation.

4           ME. FREDETTE: That is correct.

5           MEMBER ABDEL-KHALIK: All right.

6           MEMBER BROWN: Thank you.

7           ME. FREDETTE: Just so we are all clear  
8           here, we have talked about, or previously, during  
9           Terry Jackson's presentation on AP1000, we talked  
10          about the RAI process. That is strictly a licensing  
11          mechanism.

12                    When we are talking about DAC inspection,  
13                    in theory, we are talking about activities that are  
14                    done post-COL in the construction phase, and the  
15                    mechanism that we use for the review here is the  
16                    inspection process. So RAIs no longer apply.

17                    In inspection space, we have a similar  
18                    type mechanism, but it is instantaneous. We have  
19                    interface with the licensee on an immediate basis  
20                    because we are face-to-face with them during the  
21                    inspection, and findings or issues that are identified  
22                    in the inspection process are dispositioned  
23                    accordingly per the enforcement process, if it  
24                    applies, or the inspection finding process that we  
25                    have. And I will talk a little bit about manual

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Chapter 0613, which is our mechanism to do that.

2 MEMBER ARMIJO: In this process, let's  
3 take Charlie's issue of independence. You have a  
4 finding like that. How is it resolved? How does it  
5 get corrected in a way that is satisfactory, meets all  
6 the safety findings?

7 ME. FREDETTE: The inspection team or the  
8 inspectors, assume the inspectors have identified this  
9 issue. There's a problem with how the independence  
10 characteristic was implemented. That is dispositioned  
11 in accordance with our guidance. Our manual Chapter  
12 613 is the guiding document for inspection,  
13 construction inspection and construction inspection  
14 findings.

15 It would be dispositioned. There would  
16 probably be enforcement that would come out of that.  
17 But, ultimately, the licensee is responsible for  
18 remediating the implementation to correct the problem.

19 MEMBER ARMIJO: So they would submit some  
20 sort of documents or plans to correct the problem --

21 ME. FREDETTE: That's right.

22 MEMBER ARMIJO: -- which might involve the  
23 staff here?

24 ME. FREDETTE: Yes. We would, assuming we  
25 identified it during an inspection, that would be held

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 over as something we would follow up on at a later  
2 date to make sure that they corrected the deficiency.

3 The enforcement would still apply, but ultimately it  
4 is up to the licensee to remediate, make the  
5 corrective actions. Ultimately, the licensee's  
6 objective is they want to complete all these ITAAC, so  
7 that they can operate.

8 MEMBER ARMIJO: I understand that.

9 CHAIRMAN BLEY: Dr. Armijo had something  
10 that I want to go back to, and then we will go to Joy.

11 The way you said it, Sam, I don't think is  
12 the way we have been told this is going to go forward.

13 The inspection team will include technical expertise.  
14 Probably some of the people we have seen here would  
15 be involved.

16 ME. FREDETTE: Yes, I am going to talk  
17 about that a little bit.

18 CHAIRMAN BLEY: It is not that it would be  
19 an inspector who is not --

20 MEMBER ARMIJO: No, I understand that.

21 CHAIRMAN BLEY: Okay.

22 MEMBER ARMIJO: They would pull in, in  
23 addition to the inspection people, they would bring in  
24 experts from the staff for --

25 CHAIRMAN BLEY: Yes, both for the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 inspection and for looking at whatever comes back.

2 And, Joy, you had something?

3 ME. FREDETTE: Just a point to make about  
4 inspections, I, too -- Terry Jackson mentioned he is  
5 an inspector -- I, too, am an inspector. It has been  
6 my experience with the agency that, as an inspector,  
7 whether I am by myself or as part of a team, I have  
8 the resources of the entire agency at any given time  
9 to help with disposition of issues, identification of  
10 issues, what the issues mean, how we are going to  
11 handle, and what they will ultimately mean to the  
12 licensee. And that is true for any inspection ongoing  
13 now.

14 We always have the ability to bring the  
15 right expertise and the right level of size,  
16 resources, or whatever, we have the ability to bring  
17 that to bear on any particular issue at any time  
18 during an inspection.

19 Yes, ma'am?

20 MEMBER REMPE: Since this is a new  
21 process, what if during the inspection process you  
22 find that they meet the ITAAC, but maybe that the  
23 ITAAC wasn't sufficient. So, basically, they are not  
24 in violation. They met the criterion, but the  
25 criterion was not adequate. What would be the process

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 then?

2 *ME. FREDETTE: Well, in other words, the*  
3 *ITAAC was --*

4 *MEMBER REMPE: Wasn't sufficient.*

5 *ME. FREDETTE: -- wasn't sufficient. But,*  
6 *back in licensing, as part of the licensing review,*  
7 *the staff would have determined that the ITAAC was*  
8 *sufficient as part of the licensing --*

9 *MEMBER REMPE: But I'm saying, what if it*  
10 *is because it's --*

11 *ME. JUNG: In those cases, staff will*  
12 *evaluate that. For example, there was an ITAAC that*  
13 *is relevant to independence. Let's use that as an*  
14 *example. ITAAC was met. However, there was another*  
15 *issue related to some relevant issue out beyond the*  
16 *ITAAC. The agency would evaluate that issue. The*  
17 *agency has its own separate process to determine how*  
18 *significant that is, if we need to invoke any other*  
19 *ways, other methods to follow to ensure that safety*  
20 *issue is appropriately addressed.*

21 *ME. SANTOS: Laura?*

22 *MS. DUDES: I just want to add, because I*  
23 *think it is an important point, and I just want to*  
24 *make sure we have a lot of clarity.*

25 *And by the way, since we are all doing it,*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I was an inspector, too, for eight years.

2 (Laughter.)

3 All right. So that was a really good  
4 question. What teed this off was Tom's bullet on no  
5 impact on the safety finding. And what he means is  
6 the safety finding that we make at the DCD stage.

7 When an inspector in the field finds that  
8 a licensee -- and this includes the current; we have  
9 104 operating reactors with a licensing basis right  
10 now. Any one of our inspectors finds that they are  
11 not in conformance with that licensing basis, the  
12 licensee has two choices. They make a change to make  
13 sure they are in conformance with that licensing basis  
14 or they submit an amendment for the staff to review.

15 But compliance with the licensing basis is  
16 always the licensee's responsibility. Being outside  
17 of compliance is a violation and it does not meet our  
18 regs.

19 I guess, with your one example, I just  
20 wanted to, if we find that there is an issue  
21 associated with the design, and maybe the ITAAC wasn't  
22 as clear, again, compliance with their licensing basis  
23 and the regulations is always their responsibility.  
24 So we would always have a mechanism to pursue a  
25 corrective action if there was a safety issue

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 associated with any finding that they find, whether it  
2 is ITAAC-related.

3 We will have other inspections during  
4 construction that won't be related to ITAAC, and if  
5 they are not in compliance with the regulations or the  
6 licensing basis, they must bring that plant into  
7 compliance, and we have regulatory mechanisms to do  
8 that.

9 MEMBER BROWN: Let me amplify that, and I  
10 won't name the particular project that was involved at  
11 one of the early meetings in which I participated  
12 relative to one of the digital I&C certification  
13 processes.

14 When asked about establishing  
15 independence, the answer was they met the IEEE 603  
16 because they were electrically-isolated, period.  
17 Fiberoptics was the answer; they were electrically-  
18 isolated, and therefore, they met the IEEE 603  
19 requirements.

20 And when pushed to answer, based on,  
21 obviously, difference of opinion, there was what I  
22 would call a relatively stubborn reaction and that  
23 that's the way it is; we're not required to provide  
24 any other information, period.

25 That has subsequently changed, and there's

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *been considerable more -- that's the difficulty. If*  
2 *you look at IEEE 603 and some of the requirements,*  
3 *they have been in the past, because in the old analog*  
4 *world there were certain meetings, it was understood,*  
5 *and it worked out just fine. It is not the same in*  
6 *the digital computer-based world.*

7 *So, the whole issue -- and there's a*  
8 *number of those issues that are like that -- so it can*  
9 *get fuzzy if the acceptance criteria or the ITAAC does*  
10 *not include sufficient specificity, as Joy suggested,*  
11 *and then you get down. Now you are trying to set up a*  
12 *plant. The plant is being built. They want to go*  
13 *operate. Now you find, oh-oh, it doesn't meet it.*  
14 *Yes, I meet it; I've got my fiberoptic lines here.*  
15 *That's all that was in there, and therefore, I can*  
16 *proceed.*

17 *And that is not a satisfactory answer, but*  
18 *now the agency is faced with saying you can't operate.*

19 *MEMBER ABDEL-KHALIK: Let's continue,*  
20 *please.*

21 *MEMBER BROWN: Go ahead. Thank you, Said.*

22 *ME. FREDETTE: Where did I leave off? The*  
23 *fourth bullet.*

24 *Our DAC inspection is focused on the*  
25 *fundamental design characteristics, key attributes of*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the system, the development processes that are in  
2 place, and the acceptance criteria that are in the  
3 ITAAC, which, hopefully, we would determine are  
4 acceptable acceptance criteria in the first place.

5 The inspections are generally initiated  
6 and driven by the applicant's development schedule and  
7 key milestones.

8 Next slide, please.

9 This graphic just depicts a typical or  
10 conceptual development schedule and timeline and  
11 where the DAC inspections would fall. It basically  
12 mirrors the typical development life cycle. It is  
13 meant to show that DAC inspections are conducted, or  
14 would be conducted, all along the key milestones in  
15 lockstep with a licensee's schedule, and that all the  
16 DAC would be inspected well before the 103G finding.

17 ME. SANTOS: This is this ESBWR, I just  
18 want to point out.

19 ME. FREDETTE: No, this is generic.

20 ME. SANTOS: No, no, no. I understand,  
21 but like we discussed earlier with the AP1000, their  
22 DACs were earlier phases and the original ITAAC. In  
23 the case of ESBWR --

24 ME. FREDETTE: Yes, this would be a  
25 reflection of the --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1            *MEMBER ABDEL-KHALIK: Post-COL.*

2            *ME. SANTOS: Correct.*

3            *ME. FREDETTE: Post-COL, yes, sir.*

4            *Next slide then. Thank you.*

5            *Our approach, all DAC are inspected. So*  
6 *all digital I&C DAC would be inspected. We use a*  
7 *synergistic team concept. It is Region II Center for*  
8 *Construction Inspection has the lead for all ITAAC*  
9 *inspection. But for DAC inspection, we have augmented*  
10 *the Region II inspection staff with the technical*  
11 *staff here at headquarters. In all cases, that*  
12 *expertise would be the same expertise that was engaged*  
13 *in the licensing review.*

14           *MEMBER ABDEL-KHALIK: I do understand*  
15 *that, by augmenting the inspection team with*  
16 *individuals who have been intimately involved in*  
17 *making the safety case, sort of allows for any*  
18 *deficiencies in the procedures to be sort of taken*  
19 *care of because these people have the direct*  
20 *experience associated with the system they are*  
21 *involved in inspecting, because they went through it*  
22 *during the review process. But is that a*  
23 *vulnerability?*

24           *ME. FREDETTE: Well --*

25           *MS. DUDES: Can I just try this, Tom, for*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 now?

2 *ME. FREDETTE: Yes.*

3 *MS. DUDES: I understand, and in terms of*  
4 *the inspection teams, yes, the vulnerability is that*  
5 *you have what, a limited number of experts on the team*  
6 *or?*

7 *MEMBER ABDEL-KHALIK: No, if this guy*  
8 *decides to get a job with GE.*

9 *(Laughter.)*

10 *MS. DUDES: And I understand your concern,*  
11 *and there is an absolute to that. But, even in the*  
12 *current design, today we do really in-depth design*  
13 *inspections at the current fleets, and they will go*  
14 *out and they will delve into the design documents.*  
15 *And again, there is an expectation that all of the*  
16 *inspectors on the team have the level -- we are not*  
17 *going to have a pump engineer go on an I&C inspection.*

18 *MEMBER ABDEL-KHALIK: I think you missed*  
19 *the point, Laura.*

20 *MS. DUDES: And they are required to*  
21 *prepare and go through the DCD and through all these*  
22 *documents. They spend a lot of time preparing --*

23 *MEMBER ABDEL-KHALIK: Laura, I think you*  
24 *missed the point.*

25 *MS. DUDES: Okay.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           ME. SANTOS:     Said, Mr. Chairman, if I  
2     could offer, I think the answer is, yes, it is a  
3     vulnerability. As we go through them, we need to  
4     leverage the lessons learned and somehow capture that  
5     knowledge and make it more standardized for the future  
6     reviewers, whomever they be, to be able to leverage  
7     that.

8           Because, you know, today the scope, the  
9     guidance we are using is pretty much the same. Okay?

10     So, as we go through the first few ones, we need to  
11     consider. That would be my individual recommendation.

12           MEMBER ABDEL-KHALIK:     I mean the  
13     underlying reason for the question is a document dated  
14     September 23rd, 2010, entitled, "Draft Procedure for  
15     Digital Instrumentation and Control Design Acceptance  
16     Criteria Inspection".

17           And the question that came to mind, which  
18     I mentioned earlier, you make the safety case based on  
19     a lot of information in a lot of different documents  
20     at many different locations that vary depending on  
21     which DAC you are talking about.

22           And therefore, to me, it would just seem  
23     like an incredibly daunting task to write a single  
24     general procedure that allows an inspection team to  
25     touch and evaluate each and every source of

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 information on which the safety case was made.

2 And that to sort of compensate for any  
3 deficiencies in the procedure, one can argue that you  
4 are using the same people who were involved in making  
5 the safety case to also be involved in the inspection  
6 because they do remember where all that information  
7 is. But that, in my view, is a vulnerability. It  
8 doesn't fully compensate for any deficiencies in the  
9 procedure.

10 MS. DUDES: Okay. And I was going to ask  
11 you, I wanted to just capture that concern. So  
12 vulnerability associated with compensating the  
13 procedure, because I didn't get that the first time.

14 MEMBER ABDEL-KHALIK: Right.

15 ME. SHUAIBI: Let me, I want to make sure,  
16 Doctor -- this is Mohammed Shuaibi from the staff -- I  
17 want to make sure we are not misleading you here.

18 Recognizing that this may be many years  
19 out, we are not suggesting to you that Dinesh is going  
20 to be here 30 years going out on these inspections.  
21 That is not what we are suggesting here. Hopefully,  
22 he will be here and, hopefully, he will be doing a lot  
23 of good work for us, but that's not what we're --

24 MEMBER ABDEL-KHALIK: And I didn't mean  
25 that in a personal sense.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (Laughter.)

2 You know, vulnerabilities in general.

3 ME. SHUAIBI: Right, right. And in fact,  
4 I mean we have the same situation with it, if many  
5 years down the line we have an amendment that comes in  
6 to change something at the plant and we don't have the  
7 same staff that did the original review.

8 What we are suggesting, and what Tom is  
9 saying, is we will have the same level of expertise  
10 with us on these inspections. So it is people with  
11 that level of expertise that know enough to know where  
12 to look and what to do, and the inspection procedures  
13 will guide them in terms of what to look at and how to  
14 find the information.

15 MEMBER ABDEL-KHALIK: Right.

16 ME. SHUAIBI: So we don't see that -- I  
17 mean this is how we do business, and this is how we do  
18 licensing, license amendment reviews. This is how we  
19 do inspections today.

20 And on this one, Tom is going, he is going  
21 to try to address how we are going to write these  
22 procedures and get out there and do these inspections,  
23 so that we are confident that we are doing the right  
24 amount of work in this area.

25 MEMBER ABDEL-KHALIK: But this is an

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *incredible burden --*

2 *ME. SHUAIBI: Yes.*

3 *MEMBER ABDEL-KHALIK: -- to demonstrate*  
4 *that a single generic procedure --*

5 *ME. SHUAIBI: Of course.*

6 *MEMBER ABDEL-KHALIK: -- will be able to*  
7 *provide inspectors with the guidance that would allow*  
8 *them to do the evaluation of all the information on*  
9 *which the safety case was based for all the DAC, for*  
10 *all the Design Centers.*

11 *ME. SHUAIBI: And I think we are going a*  
12 *little too far because, you know, the first procedure*  
13 *is for the digital I&C, and it has six appendices to*  
14 *it, six attachments. So I think when we say a single*  
15 *procedure for all of DAC, I think we are stretching it*  
16 *too far.*

17 *MEMBER ABDEL-KHALIK: Yes.*

18 *ME. SHUAIBI: And I am going to come back*  
19 *to Tom because I do really want him to get through his*  
20 *presentation.*

21 *MEMBER ABDEL-KHALIK: Yes, sir.*

22 *ME. SHUAIBI: But the other thing that I*  
23 *would suggest, and that is why we are suggesting that*  
24 *we are going to be sending these procedures to the*  
25 *Committee for review and we will be engaging with you*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 on the adequacy of the program that we are setting up  
2 for inspecting DAC. They are coming to you for  
3 review. We look forward to those interactions and the  
4 comments that we will get back from you on the  
5 inspection procedures and how we will carry out those  
6 inspections.

7 MEMBER ABDEL-KHALIK: Thank you.

8 ME. SANTOS: Okay. And, Said, like I was  
9 saying, similar to other, Mr. Chairman -- (laughter)  
10 -- sorry.

11 MEMBER ABDEL-KHALIK: It is perfectly  
12 fine.

13 ME. SANTOS: I apologize.

14 Like in other items for this review, we  
15 develop staff training. We develop additional  
16 guidance. We expect to do the same as we get better,  
17 work through that process, and I think that is an  
18 important component, in addition to having sound  
19 inspection procedures.

20 ME. FREDETTE: And just to add onto that,  
21 you know, we are engaged in a DAC inspection effort  
22 with South Texas right now. Yes, it's no small effort  
23 to get together this procedure. That's why it has  
24 taken me a year just to get to this stage, and the  
25 procedure is not complete yet. You will notice it is

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 a draft and you have only got half of it. The final  
2 portions of it are still in development.

3 But the effort that we have put into the  
4 process and the procedure, and our efforts that we are  
5 undertaking with the South Texas Project, as we go  
6 along, we are still in the early infancy stages of  
7 this process, and as we go along, our expectation is  
8 that we will iron out a lot of the nuance out of this;  
9 we will identify what the proper level of effort is  
10 going to be, all of those things. It is still a work-  
11 in-progress, I guess is the point to make.

12 I wasn't done with that slide.

13 (Laughter.)

14 As I mentioned, we are using that team  
15 approach with our South Texas Project effort right  
16 now. So far, we have completed one inspection back in  
17 June of this year.

18 The results of using the technical  
19 expertise that exists here at headquarters in  
20 partnership with experienced inspectors in the field  
21 seems to work very well.

22 The inspection procedure that we have been  
23 talking about, it generally mirrors a typical life  
24 cycle. It has a lot of flexibility built into it.  
25 And the inspection procedure doesn't exist in a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 vacuum, and it is never used quite by itself. There  
2 are always other references that could be called into  
3 or brought into play as an inspector is going through  
4 the inspection planning process.

5 And finally, inspection activities we  
6 envision are equivalent to or very similar to audit  
7 activities. And just a point to make here, and this  
8 is sort of anecdotal, but during our first inspection  
9 that we conducted back in June, at the latter stages  
10 of that inspection, the team was discussing whether we  
11 would have done anything different during the  
12 inspection if all the information had been provided to  
13 us during licensing. And the answer was no. What we  
14 had done during the inspection was equivalent to what  
15 we would have done if all that information had been  
16 provided not in an inspection environment, but in a  
17 licensing environment. So that sort of gives us  
18 confidence that we are on the right track here.

19 MEMBER ARMIJO: What kind of DAC was that?  
20 What kind of system?

21 ME. FREDETTE: That was South Texas  
22 Project, Unit 3 and 4, I will call it project-level,  
23 South Texas Project-level planning phase activities.  
24 This was the South Texas Project high-level planning  
25 documents for their digital system development.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   MEMBER ARMIJO:   Okay.

2                   ME.   FREDETTE:       For all their digital  
3 system vendors.

4                   MEMBER BROWN:       Hardware as well as  
5 software? Is that an overarching one or is just a  
6 software management --

7                   ME.   FREDETTE:       It was overarching,  
8 software and hardware.

9                   MEMBER BROWN:   Okay.

10                  ME.   FREDETTE:   Now just to tag along with  
11 the example that Dinesh talked about earlier, this is  
12 the ESBWR example. This is the DAC/ITAAC related to  
13 single-failure criterion. It is ITAAC 2.2.15-2(8a).  
14 The design commitment is listed there. It is the  
15 single-failure criterion.

16                  The inspection test and analyses is that  
17 an inspection of the software project design phase  
18 summary Baseline Review Record shows that an FMEA has  
19 been completed. And it was designated by GE-Hitachi  
20 as Design Acceptance Criteria.

21                  Next slide.

22                  Here's the acceptance criteria. The  
23 Baseline Review Record shows that an FMEA has been  
24 completed, and it shows that the software project's  
25 safety-related functions can be performed in the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 presence of, and there are specific items that are  
2 identified as the acceptance criteria.

3 And our procedure, the guidance is  
4 provided in Appendix 3. It is on the very last page.

5 If anyone has a copy of that draft procedure, it is  
6 on the very last page. It is the failure analysis  
7 portion of the guidance from the design phase safety  
8 analysis.

9 It basically says that an FMEA or other  
10 failure analysis, equivalent failure analysis, should  
11 be performed to ensure if single-failure requirements  
12 associated with the system safety analysis assumptions  
13 are confirmed.

14 The FMEA should include system  
15 architecture to ensure that design principles of  
16 redundancy and independence have been incorporated and  
17 that single-failure requirements are met.

18 And then, there are some attributes that  
19 the inspector can verify: that all failure modes for  
20 the system/software were identified; that the impact  
21 on the system was evaluated, and provisions for  
22 compensatory measures were identified and included.

23 This guidance was incorporated from --

24 MEMBER BROWN: Which page is it?

25 ME. FREDETTE: A3-7.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   CHAIRMAN BLEY:    The second-to-last page,  
2                   Charlie.

3                   MEMBER BROWN:   Oh, okay.  I was looking at  
4                   the page that says A3-8.  So I was focusing on the  
5                   page here.

6                   ME.  FREDETTE:     The guidance there was  
7                   incorporated from NUREG 6101, which is software  
8                   development process, and then IEEE 352, which is an  
9                   IEEE standard that deals with reliability.

10                  ME.  SANTOS:    And those standards have a  
11                  lot into them also.  So it is the combination of that  
12                  together that drives us, Charlie, to try to answer  
13                  your earlier question about what is it that you are  
14                  going to be doing once you are presented with that  
15                  FMEA.

16                  So, hopefully, this gives the members a  
17                  better appreciation for this particular example.

18                  ME.  FREDETTE:   Now the inspector would  
19                  rely on the guidance that is contained in this  
20                  procedure, other guidance that is available to him,  
21                  and his own expertise, his own expertise related to  
22                  failure modes and how they are analyzed.

23                  MEMBER STETKAR:  People have said I have  
24                  been notably quiet, and I have.

25                  (Laughter.)

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           Your point No. 1 there, "All credible  
2 failure modes for the system/software were  
3 identified." And you made ample reference to guidance  
4 in IEEE standards and all of that kind of stuff.

5           I'm not aware of any IEEE standards that  
6 address software failure modes. So, who determines  
7 that, indeed, all credible failure modes have been  
8 identified? Who makes that value judgment? Does the  
9 inspector?

10           ME. SANTOS: The inspector --

11           MEMBER STETKAR: Is there a list?

12           ME. SANTOS: No.

13           MEMBER STETKAR: Who makes -- and for each  
14 individual set of hardware and software for each of  
15 the Design Centers, which, indeed, will have a  
16 different mix of individuals. So who makes that? It  
17 says "all", which is a big word -- (laughter) --  
18 "credible", which is also a very big word, "failure  
19 modes", which is an ill-defined term, "for the  
20 system", which I'm not quite sure it is, "/software  
21 were identified." Who makes that determination and  
22 how is it made, so that you can say, "Yea, verily, we  
23 certify that, indeed, this was done and it's  
24 acceptable."?

25           ME. SANTOS: The right expert on the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 inspection team and --

2 MEMBER STETKAR: Oh, I hear those words.  
3 Who does it and how is it done?

4 ME. SANTOS: Okay. I can take a stab at  
5 it.

6 I agree, "all credible", it could be --

7 MEMBER STETKAR: That's what it says.  
8 This is the procedure. So, if I'm an inspector, I'm  
9 going to follow this.

10 ME. SANTOS: I'm going to give you a  
11 little practice here. What I will do if I'm it on the  
12 team, for example?

13 It is not only looking at the specific  
14 design, so I can narrow the universe to the specific  
15 application, I have to look at the literature out  
16 there, the professional literature associated with  
17 that particular technology application. I will have  
18 to look at any operation experience, domestic and  
19 international, that might be --

20 MEMBER STETKAR: There isn't any.

21 ME. SANTOS: There's some.

22 MEMBER STETKAR: Well, oh, sure, digital  
23 feedwater systems, little feedwater systems.

24 ME. SANTOS: And most critical, also, for  
25 the ones that are in my expertise, what are the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 mitigations? Do I have any other system features that  
2 also help --

3 MEMBER STETKAR: No, that doesn't say, do  
4 I have something that saves me --

5 ME. SANTOS: Oh, okay, I understand.

6 MEMBER STETKAR: -- in the event that this  
7 thing goes belly up? That's a different issue.

8 ME. SANTOS: Okay. Sure, sure, sure.

9 MEMBER STETKAR: This says that I did a  
10 comprehensive, integrated failure modes and effects  
11 analysis --

12 ME. SANTOS: The answer is I will pull out  
13 previous FMEAs.

14 MEMBER STETKAR: There aren't any.

15 ME. SANTOS: Yes, I can show you the  
16 AP1000.

17 MEMBER STETKAR: Software?

18 ME. SANTOS: Software is covered at some  
19 level, not -- if we look at software, I would not --

20 MEMBER STETKAR: "All credible failure  
21 modes" --

22 ME. SANTOS: I would have to look at  
23 software analysis, which is kind of the,  
24 quote/unquote, "software FMEA equivalent". Some of  
25 them are very weak. Okay?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I will bring my own personal experience  
2 with my own --

3 MEMBER STETKAR: I have made my point.  
4 Okay, I've made my point.

5 ME. SHUAIBI: If I may --

6 MEMBER STETKAR: Yes.

7 ME. SHUAIBI: -- I just want to add these  
8 are draft inspection procedures. I think you have a  
9 point from Tom that we are implementing these, trying  
10 to implement them and use them and see what that  
11 means. The word "all", I guess maybe we need to take  
12 that back and think about it.

13 But let us at least walk you through the  
14 process in terms of what we would do and not focus so  
15 much on the word "all", if that is okay with you. I  
16 mean I would rather walk you through how we would do  
17 it.

18 MEMBER STETKAR: That's fine. My point is  
19 that the mix in the expertise, the diversity of "I's"  
20 in experience who are looking at this integrated  
21 design at the point at which it is inspected, if you  
22 want to use that term, is very, very important.

23 ME. SHUAIBI: We agree.

24 MEMBER STETKAR: Because I don't care what  
25 mix of individuals you have, they are not going to

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 have that diversity of expertise, especially -- and  
2 Said mentioned something earlier -- especially if a  
3 number of those individuals have lived with all of the  
4 detail for the last -- pick a number of how many years  
5 you have lived with it -- because you already know  
6 what you know. You already know what you are looking  
7 for.

8 And because of that, you are looking for  
9 the specific things that you know you need to look  
10 for. You haven't thought about looking for other  
11 things.

12 So that is the only point of this  
13 inspection process. And I focused on "all" and  
14 "credible" because they are trigger words, but I am  
15 trying to get that message across.

16 ME. TANEJA: Yes, I agree with you on that  
17 expertise level. I mean, you know, from our  
18 experience, my personal experience, a lot of this  
19 expertise comes from working. I mean, if you find an  
20 individual who has worked with a digital I&C platform  
21 for "X" number of years, you know, he slept with it;  
22 he got called in the middle of the night with X, Y, Z  
23 problem, right? So they know what is the failure  
24 mechanism that got them and all that type of thing.

25 And also, some of these vendors -- I think

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I visited Triconex. They keep a very good record of  
2 all their anomalies and the failures that got  
3 reported. It was a wealth of information that I  
4 learned from them just by going to a one-week  
5 training.

6 The question was asked, "You know, hey,  
7 what did you guys learn from the last 20 years with  
8 this thing?" And it is an amazing amount of  
9 information that is out there, right?

10 So I agree with you. I think people need  
11 to get familiar with those platforms to that level to  
12 be able to inspect them.

13 ME. SANTOS: And I agree. We will take  
14 the comment back on "all credible". I mean there is  
15 no way we can find all the systemic failures on those,  
16 what other people call them --

17 MEMBER BONACA: But you can use the words  
18 that there is reasonable assurance --

19 ME. SANTOS: Correct.

20 MEMBER BONACA: Okay. I mean use that.

21 ME. FREDETTE: As part of this example,  
22 there is a companion ITAAC for that ITAAC 8a which was  
23 the DAC for single-failure criterion. This is a  
24 standard ITAAC, 2.2.15-2(8b).

25 The acceptance criteria here just says

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that an installation phase report documents that the  
2 as-built testing confirms the FMEA results. In other  
3 words, there will be testing done in the installation  
4 phase that will confirm the FMEA, what the FMEA says.

5 And in this particular case, it would be  
6 the inspectors who would be monitoring the testing  
7 would reconcile results of the ITAAC inspection with  
8 any previously-documented results from the DAC  
9 inspection that we just talked about.

10 In a realistic sense, the DAC inspection  
11 might have been done many, many months before we get  
12 to this particular test.

13 CHAIRMAN BLEY: The discussions earlier  
14 today, especially some of the ones Charlie got  
15 started, about ITAAC, a simpler ITAAC, the test,  
16 raised the point that the acceptance criteria in the  
17 ITAAC in Tier 1 don't tie in all the requirements that  
18 are off in the DCD and the topical and other places.

19 We have got the same problem with at least some of  
20 those that we have with the DAC, in that somebody with  
21 the expertise to know where all of that lies somehow  
22 needs to make sure that gets factored into the test,  
23 like the one example of the background load on the  
24 processors.

25 If it is not in the ITAAC, but you do have

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to meet it, how does that get picked up? And is the  
2 integrated team going to lay out the requirements for  
3 those kinds of tests as well?

4 *ME. FREDETTE:* Dennis, those kinds of  
5 features to the inspection are developed during the  
6 inspection planning process.

7 *CHAIRMAN BLEY:* Okay.

8 *ME. FREDETTE:* As an example, when we did  
9 this planning phase inspection back in June --

10 *CHAIRMAN BLEY:* Yes.

11 *ME. FREDETTE:* -- South Texas made  
12 available to us over 60 documents that the inspection  
13 team was able to use to develop the inspection plan  
14 and the scope of what they were actually going to look  
15 at on this particular inspection.

16 *It is expected that inspection planning is*  
17 *no small effort. Inspectors can take up to two, three*  
18 *weeks at a time planning all the things that they*  
19 *need, all the tools that they need in their little*  
20 *pouch that they are going to use when they go out and*  
21 *do an inspection that might last a day and a half or*  
22 *two days maybe.*

23 *Those types of things are expected of the*  
24 *inspectors. And the team working together identifies*  
25 *the items that they are going to need and the*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 resources that they are going to have to bring to bear  
2 from either a documentation standpoint or other  
3 resources, other personnel that they are going to need  
4 and some of the specific features that they are going  
5 to want to look at and be mindful of.

6 CHAIRMAN BLEY: Okay. Well, I think we  
7 need to hear more about this because this gets close  
8 to what Said has raised several times today. If you  
9 have a general inspection procedure, how does that  
10 roll into some kind of a detailed plan that lays out  
11 all of these requirements for each of the ITAAC that  
12 need that kind of examination to make sure that you  
13 are covering all of the requirements that are buried  
14 elsewhere?

15 ME. BEARDSLEY: If I may, this is Jim  
16 Beardsley from the Division of Construction  
17 Inspection.

18 We are working with the Region to identify  
19 those families of ITAAC where a general inspector  
20 wouldn't innately have the background to go after that  
21 particular area. If it is pouring concrete, we have  
22 concrete-trained inspectors. If it is a digital I&C,  
23 for instance, we are identifying those families today.

24 We are working with the technical staff  
25 here at headquarters to build the strategies for

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 inspecting those ITAAC and documenting the -- we are  
2 trying to estimate the number of hours, the inspection  
3 procedures we will look at, the additional  
4 documentation we will use in preparation for that.

5 So we are trying to identify those  
6 upfront, so that when we get to that inspection, we  
7 have already done a lot of that background work; they  
8 know who to call on. And then, we will, the Division  
9 of Construction Inspection will coordinate those  
10 inspection hours with the applicable Branch Chiefs.  
11 So we will work with the Digital I&C Branch to make  
12 sure they have the right people available to do that  
13 inspection at the right time.

14 ME. SANTOS: And, Mr. Chairman, we are not  
15 starting from zero regarding the mapping between the  
16 DCD and the ITAAC, because it is the applicant's  
17 responsibility to close the ITAAC and the DAC. So  
18 they would have had to generate their case for the  
19 closure. Okay?

20 CHAIRMAN BLEY: Right.

21 ME. SANTOS: So you have two sets of teams  
22 that will have to converge at some point on what are  
23 the critical characteristics, tests that ought to be  
24 verified.

25 CHAIRMAN BLEY: Not to beat a dead horse,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 but, boy, that would be a lot easier if that had all  
2 been built into the ITAAC.

3 MEMBER ARMIJO: Yes.

4 CHAIRMAN BLEY: Back to you, Tom.

5 ME. FREDETTE: We agree, and the  
6 convergence that Dan is talking about is the  
7 inspection element and then what the licensee is doing  
8 on the licensee side to bring their forces together to  
9 make sure they complete the ITAAC and meet the  
10 acceptance criteria in the ITAAC specifically.

11 ME. SANTOS: If I may, I have Gerry Wilson  
12 from Licensing. The fact that we put more detail on  
13 the ITAAC/DAC could bring some additional regulatory  
14 implications that I would like for him to briefly  
15 explain to the members, just for information.

16 CHAIRMAN BLEY: It is always good to hear  
17 from Mr. Wilson.

18 ME. SANTOS: Yes, and I was missing your  
19 voice.

20 (Laughter.)

21 ME. WILSON: Gerry Wilson, Office of New  
22 Reactors.

23 What Dan is talking about is the actual  
24 process of determining the level of information that  
25 goes into Tier 1 and also in the acceptance criteria.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1       So you couldn't simply reference down from the  
2       acceptance criteria to supporting documentation in  
3       what we refer to as Tier 2 in the Design Control  
4       Document because that draws all of that information  
5       now up to Tier 1, and it has to be treated and handled  
6       as Tier 1 information, which has pertinence associated  
7       with it and restrictions on flexibility. You have to  
8       keep all of that in mind.

9               So it is understood that there is  
10       information in Tier 2 in the relevant subject area  
11       that supports the ITAAC and the acceptance criteria.  
12       That is all understood by the people who wrote it and  
13       the people who are going to be reviewing it and the  
14       people who are going to be inspecting it. That is  
15       just part of the process.

16               So, back to their point that we are using  
17       knowledgeable inspectors and those inspectors know  
18       where to go to find the relevant information to aid  
19       them in performing that inspection. All those details  
20       don't need to be in the acceptance criteria.

21               CHAIRMAN BLEY: Thank you.

22               MEMBER BROWN: I disagree with that. The  
23       argument is that the designer is not going to be  
24       restricted. If you put it in there, then he's got  
25       restrictions on him. And he can do anything he darned

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 well pleases. And therefore, it is just this big  
2 whitewash when it comes to looking at acceptance  
3 criteria and what he is going to be doing, and you  
4 can't track it from design to design to design.

5 So I flat disagree with that in the  
6 strongest terms I can even -- I'm trying to say it  
7 nicely.

8 (Laughter.)

9 But I just want to make sure that having  
10 no acceptance criteria is not a valid approach to  
11 doing anything because it stifles innovation or  
12 restricts things because technology may be changing,  
13 or whatever argument you may be making. That is weak.

14 I'm almost finished maybe --

15 CHAIRMAN BLEY: I think we will go back to  
16 them.

17 MEMBER BROWN: I'm sorry. Excuse me. I  
18 will stop now. Is that what you are asking me to do?

19 CHAIRMAN BLEY: That's what I'm asking you  
20 to do.

21 MEMBER BROWN: Then I will stop now.

22 CHAIRMAN BLEY: Tom?

23 ME. FREDETTE: Assuming that we have  
24 conducted an inspection, the inspections are  
25 documented using the guidance that I talked about

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 earlier. This is manual Chapter 0613. This is where  
2 findings from the inspection are dispositioned and  
3 appropriate conclusions are made, and enforcement, if  
4 enforcement is applicable. This is where those  
5 determinations are made.

6 The inspection report is always docketed  
7 as usual. Inspection details are archived in our  
8 CIPIMS, which is a Construction Inspection Program  
9 Information Management System. It is a database, a  
10 repository for all inspection results in construction  
11 inspection space.

12 The data that is in CIPIMS will be used by  
13 the staff -- (interruption by electronic equipment  
14 noises)

15 CHAIRMAN BLEY: Just try to go ahead.  
16 They have got to clean it up back in the booth there.

17 ME. FREDETTE: The data that is in CIPIMS  
18 will be used by the staff to support the ITAAC closure  
19 process.

20 And speaking of ITAAC closure, just to  
21 walk through how ITAAC closure is accomplished, it is  
22 incumbent upon the licensee to complete the DAC or any  
23 ITAAC. The NRC always independently inspects. If  
24 inspections are done, the licensee will submit an  
25 ITAAC completion letter.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           And just as an example, they would submit  
2 a completion letter for that ITAAC that we talked  
3 about, for the single-failure criterion DAC. The  
4 staff would review the ITAAC completion letter, which  
5 basically is a summary of everything that the licensee  
6 has done to support closure of that ITAAC. We would  
7 review the ITAAC completion letter, the CIPIMS  
8 archived information, any supporting data from any  
9 inspections that we have done previously.

10           If there's no issues with the completion  
11 letter, than the staff would issue a Federal Register  
12 notice. If there are issues, in most cases, as a  
13 matter of fact, in just about every case, we would  
14 just reject the ITAAC completion letter and send it  
15 back to the licensee. But it is The Federal Register  
16 notice that formally notifies the licensee that the  
17 ITAAC is closed.

18           And just to summarize -- I mentioned this  
19 earlier -- the DAC inspection program is still under  
20 development. We have completed one inspection. We  
21 are still in the process of compiling a lot of our  
22 lessons learned, refining our process, determining  
23 what the level of effort should be for these  
24 inspections.

25           Going forward, we are still working with

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the South Texas Project. We are projected to do three  
2 to four DAC inspections in 2011. The next one is  
3 scheduled for, we believe, the February 2011  
4 timeframe.

5 That inspection is basically to look at  
6 platform-level planning and requirements phase  
7 activities for one of South Texas' vendors. This is  
8 Toshiba. They are using the field-programmable gate  
9 array platform technology for their RPS system. So we  
10 will be looking at that in February.

11 But, as I mentioned, there are three or  
12 four other inspections that we expect to complete in  
13 2011.

14 And as we mentioned in our response letter  
15 from October 7th to the Committee, we plan to brief  
16 ACRS at key junctures in our process.

17 The inspection in February will be the  
18 first implementation of our Appendix 2 from the draft  
19 procedure that we have. So that will be an opportune  
20 time for us to brief the Committee again on our  
21 progress.

22 ME. SANTOS: I want to go back.

23 CHAIRMAN BLEY: While you are looking for  
24 it, Tom, do you have an estimate of when the remaining  
25 appendices are likely to have drafts out?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           *ME. FREDETTE: Dennis, we provided a*  
2 *schedule earlier this summer, where we provided*  
3 *Appendix 1 back in June. We made a commitment to*  
4 *provide Appendix 2 and 3 in September, which you now*  
5 *have.*

6           *CHAIRMAN BLEY: We now have, yes.*

7           *ME. FREDETTE: Appendix 4 through 6 --*  
8 *there's only six appendices -- Appendix 4 through 6*  
9 *are to be provided by December 31st.*

10          *CHAIRMAN BLEY: Okay. So that schedule*  
11 *still applies?*

12          *ME. FREDETTE: I'm developing those now.*

13          *CHAIRMAN BLEY: Okay.*

14          *ME. SANTOS: I just want to, before we*  
15 *turn it over to industry, first of all, thank you.*

16           *And I would like to go back to the third*  
17 *slide with the expected outcomes of today. I think*  
18 *your letter on the 9th was very clear, but today it*  
19 *provided additional insights, and I appreciate those.*  
20 *We have some takeaways.*

21           *But I would like to ask the members, have*  
22 *we met, also, your expectations on outcomes for today?*

23           *And if not, to work together for follow-on activities*  
24 *to do so, because I really would like to keep open*  
25 *dialog and work this through completion.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1                   CHAIRMAN BLEY:    Well, I think we will  
2 summarize toward the end of the meeting. We have one  
3 more thing to go.

4                   ME. SANTOS:    Okay.

5                   CHAIRMAN BLEY:   We will come back to that.  
6                   Of course, you know, this is a Subcommittee, so we  
7 can't speak for the whole Committee, but we will have  
8 individuals give you their feelings on today's meeting  
9 and maybe remaining questions.

10                   If we are finished with this set, any of  
11 the members have any questions you want to pursue  
12 before we are done?

13                   MEMBER ARMIJO:   Yes, I have one, and it  
14 relates to the quality and completeness of the ITAAC,  
15 so that the inspection plans don't turn into a big  
16 research program to find out where the key information  
17 has to be extracted, either from a DCD or a COL. You  
18 know, how do we assure that the ITAACs are really good  
19 enough and complete enough that the inspection  
20 planning doesn't have to be a search for requirements?  
21 And I get the feeling that they aren't.

22                   ME. FREDETTE:   Well, the FSAR is also part  
23 of the -- or the DCD, or we have a lot of documents at  
24 our disposal. And as an inspector, I can tell you  
25 that it sounds very burdensome.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   MEMBER ARMIJO: Yes, it does.

2                   ME. FREDETTE: It is really, for an  
3 experienced inspector who is experienced in the  
4 discipline, like digital I&C, it is really not as  
5 burdensome as it sounds.

6                   MEMBER ARMIJO: Okay.

7                   ME. SANTOS: I think the ultimate answer  
8 is, once we go through the process --

9                   ME. SHUAIBI: Let me add to that. This is  
10 Mohammed again.

11                   This is pretty typical, and I'll look to  
12 Tom, and he can confirm this for us here. This is  
13 pretty typical of how we do inspections, and we do  
14 inspections on the operating fleet and we do  
15 inspections in this area.

16                   But in terms of looking for documents and  
17 looking for the information, and sometimes reading an  
18 FSAR and saying, well, I need maybe some reference  
19 document within that FSAR to be made available to me,  
20 so that I could prep for this inspection that is  
21 coming up, this is pretty typical of how the agency  
22 does business.

23                   MEMBER ARMIJO: Yes, I would tend to agree  
24 with you on something that isn't as complicated and  
25 first-of-a-kind-type design. But this is truly a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *first-of-a-kind, and it is complicated.*

2 *So, anything that can be done to improve*  
3 *the quality of the ITAAC, it seems to me that it*  
4 *should be done.*

5 *ME. SANTOS: Okay.*

6 *ME. SHUAIBI: I will also add that, when*  
7 *we do the first implementation of these documents, we*  
8 *will come back and brief you. That might also add a*  
9 *little bit of how we are doing --*

10 *CHAIRMAN BLEY: Absolutely. We would like*  
11 *that.*

12 *ME. FREDETTE: Yes, that was something*  
13 *that you stipulated or that we stipulated in our*  
14 *response back.*

15 *CHAIRMAN BLEY: Right.*

16 *ME. SANTOS: And you know, that is a good*  
17 *forum to get the questions like Charlie was doing*  
18 *earlier. Where does the staff serve? Where is this*  
19 *critical characteristic?*

20 *ME. FREDETTE: A simple example that I can*  
21 *pull out is, you know, when Dinesh was going through*  
22 *his presentation, he showed you a lot of matrices and*  
23 *tables of traceability to requirements and things like*  
24 *that. That is one reason why we bring that expertise*  
25 *along on the inspection, because that expertise knows*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 how to read those tables, knows where to look, and  
2 they can impart that knowledge on the rest of the team  
3 and provide a little bit of technical guidance, so to  
4 speak.

5 CHAIRMAN BLEY: I think our worry isn't as  
6 much there as for the other Design Centers that don't  
7 even have those tables.

8 MEMBER ARMIJO: That's right.

9 ME. SANTOS: Like I said, all I could  
10 offer today is two things. You will see the process  
11 as we go through, but, also, the important element the  
12 applicants bring to this. We are not doing this from  
13 a --

14 CHAIRMAN BLEY: And we should begin to see  
15 that in February, when we --

16 ME. SANTOS: Right.

17 CHAIRMAN BLEY: Or right after February?

18 ME. SANTOS: Actually, a good thing to be,  
19 as the applicant develops what they consider their  
20 closure documents, bring it all together to bring that  
21 complete picture.

22 ME. FREDETTE: Well, requirements  
23 traceability is a common tool for development  
24 processes like this. It is really a roadmap from your  
25 functional requirements all the way to testing that

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the inspectors can use.

2 CHAIRMAN BLEY: Okay. Anything more?

3 (No response.)

4 Well, I think we will have this last  
5 presentation, and then we will have a closing session.

6 Is Ms. Keithline here?

7 MS. KEITHLINE: Yes.

8 CHAIRMAN BLEY: And you have discussion  
9 with us? Okay.

10 MS. KEITHLINE: I do.

11 CHAIRMAN BLEY: Or a presentation.

12 MS. KEITHLINE: And they told me to come  
13 up here, if that's all right.

14 CHAIRMAN BLEY: Perfect. Please do.

15 MS. KEITHLINE: Thank you, Dan.

16 CHAIRMAN BLEY: We don't have a copy of  
17 this.

18 MS. DUDES: Yes, you do.

19 CHAIRMAN BLEY: We do? Thanks, Said.

20 MS. DUDES: Dan, you just need to state  
21 for the record that you are just helping out with the  
22 slides and you're not saying --

23 ME. SANTOS: Absolutely. Thank you. Good  
24 call. I'm just hitting PageDown.

25 (Laughter.)

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   *Thank you, Laura. No, a good point.*

2                   *CHAIRMAN BLEY: Okay.*

3                   *MS. KEITHLINE: Okay. I appreciate the*  
4 *opportunity to be able to make a few brief remarks --*  
5 *they are very brief -- on behalf of the industry this*  
6 *afternoon, entering into almost this evening.*

7                   *Next slide, please, Dan.*

8                   *We will get through this pretty quickly.*

9                   *Like other industries, we are using*  
10 *digital instrumentation and control because of the*  
11 *important benefits it offers. We do understand that*  
12 *there are unique aspects of digital I&C that need to*  
13 *be addressed, and we recognize that designing digital*  
14 *I&C requires a more detailed and systematic approach*  
15 *than other systems.*

16                   *We appreciate the level of effort needed*  
17 *to resolve DAC and the importance of closing DAC*  
18 *early. But, by early, I don't mean early means that*  
19 *it has to be before the COL. By early, I mean as*  
20 *early as is reasonably practical for the given*  
21 *situation.*

22                   *And early is important. Early could be*  
23 *early in the construction process after the COL, but*  
24 *the applicants all understand that we need to be*  
25 *getting our act together to get these DACs resolved as*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 soon as makes sense in their particular situations  
2 because dragging it out increases our risk and makes  
3 your job more challenging, too, I think.

4 Okay. Where am I? Sorry about that. I  
5 just lost my place.

6 The industry does understand our  
7 responsibilities for providing oversight of DAC  
8 execution, and we also understand the importance of  
9 NRC's technically-based staff inspections. And we  
10 appreciate the work the staff has done to develop  
11 their inspection process and procedures, and the fact  
12 that they have had open technical public meetings to  
13 discuss the development of those procedures and plans.

14 That has been very helpful to us.

15 Earlier this afternoon, Laura described  
16 the three methods that can be used to resolve DAC. So  
17 that the final bullet here is that we recognize that  
18 there are multiple approaches. By that, I mean there  
19 may be different approaches in terms of whether and  
20 how many DAC are used in a particular situation and  
21 what resolution method may be appropriate in that  
22 particular situation.

23 But regardless of the DAC approach used,  
24 we do recognize that we are all doing the same thing  
25 in terms of working to the same set of regulations and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 standards. And ultimately, whether they have one DAC  
2 or 400 DAC, in the end, we envision that the level of  
3 review and the scope will be consistent among the  
4 different licensees, applicants and licensees.

5 Next slide, please. Thank you.

6 I would like to highlight just a few  
7 things that industry is doing to make sure that the  
8 DAC process will be a workable way to ensure that new  
9 plant I&C systems will be consistent with their  
10 licensing bases.

11 On a design-specific basis, vendors and  
12 COL applicants work together in Design-Centered  
13 Working Groups on issues that are generic to their  
14 particular design. Westinghouse doesn't just act  
15 alone. They act with the help and assistance from  
16 their COL applicants, the Southernns, the SCANAs, the  
17 others in that group. It is a very joint effort.

18 Within the Design-Centered Working Groups,  
19 the vendors and the COL applicants have been working  
20 together to establish DAC and the supporting Tier 2  
21 information, and in some cases also to close certain  
22 DAC, as we heard about earlier this afternoon. So  
23 that is a joint effort of those Design-Centered  
24 Working Groups, not just the vendors by themselves.

25 In true nuclear spirit, the COL applicants

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *feel ownership and responsibility for making sure the*  
2 *DAC are closed in a technically-correct and complete*  
3 *manner.*

4 *At a higher level, we have brought*  
5 *together the various Design-Centered Working Groups in*  
6 *an industry task force to focus on issues that are*  
7 *generic across Design-Centered Working Groups.*

8 *And that's the next slide, Dan. Yes.*

9 *Our Construction Inspection Program Task*  
10 *Force includes vendors and applicants representing all*  
11 *of the Design-Centered Working Groups. That is the*  
12 *Task Force that developed the guidance document*  
13 *NEI 08-01, which is our guidance, industry guidance,*  
14 *for closing ITAAC.*

15 *At our most recent Construction Inspection*  
16 *Program Task Force meeting, South Texas shared lessons*  
17 *learned from the first of their series of these pre-*  
18 *COL inspections that they did with the NRC. Our*  
19 *intent is that our Construction Inspection Program*  
20 *Task Force will provide a forum for additional lessons*  
21 *learned from that effort to be shared across the*  
22 *industry. We would like to make sure that the lessons*  
23 *learned are shared as broadly as possible, so that*  
24 *everyone benefits and can make their own execution of*  
25 *the DAC process more successful.*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   In 2011, our Construction Inspection  
2 Program Task Force is planning to revise NEI 08-01 to  
3 include additional DAC closure guidance. Some of you  
4 may recall that when we submitted Revision 3, which  
5 was endorsed by Reg Guide 1.215, I think, one of your  
6 comments was that it was a little thin on guidance  
7 related to DAC.

8                   So we recognized at the time that, with  
9 the idea of this test-out, develop the procedures and  
10 processes, and go test them out with the early South  
11 Texas inspections, that we would be learning things  
12 from that effort that can be, and should be,  
13 incorporated back into NEI 08-01. So we see that  
14 probably starting up in the 2011 timeframe, as Tom  
15 completes more of his inspection work.

16                   Okay. We are also considering writing new  
17 industry guidance for developing DAC/ITAAC closure  
18 strategies. Here, the idea would be to capture some  
19 best practice ideas for creating and maintaining what  
20 we call ITAAC closure packages. This is the package  
21 of information that the licensee maintains that really  
22 provides the basis of their case for closing or  
23 resolving the DAC or ITAAC. Dan made mention of this  
24 just a little bit ago.

25                   So, as we have been developing the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 guidance for ITAAC closure, we have started recently  
2 to discuss there are probably some good ideas, some  
3 consistent guidance that we can provide, develop and  
4 provide, so that that process for developing and  
5 implementing those packages is more consistent and  
6 addresses what needs to be addressed.

7 We have been over the last few years  
8 working very closely with NRC inspection personnel,  
9 both at headquarters and in the regions, through this  
10 effort to develop guidance for ITAAC closure and now  
11 ITAAC maintenance. And we envision continuing that,  
12 and it would also address the things unique or  
13 specific to DAC that come out of these discussions and  
14 other discussions. So we are very interested in  
15 continuing the work with all of you and any other  
16 stakeholders on making this process successful.

17 That is pretty much it. Mine were very  
18 brief remarks.

19 I just wanted to make sure that you  
20 understood or had an idea of what is going on in  
21 industry and efforts to learn from some of these  
22 experiences and provide better guidance, so that we  
23 can be more successful with this process.

24 CHAIRMAN BLEY: Okay. Thank you very  
25 much.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. KEITHLINE: Thank you.

2 Thanks, Dan.

3 CHAIRMAN BLEY: At this time, I guess I  
4 should ask if there are any members of the public in  
5 this room who would like to make a comment.

6 (No response.)

7 And I don't see any here.

8 I suppose we should also -- oh, Bill, are  
9 you still here? Bill Shack? Maybe that is who we  
10 heard leave.

11 ME. SANTOS: Is it muted?

12 MS. ANTONESCU: No, no. I think he's  
13 gone.

14 ME. SANTOS: He's gone?

15 MS. ANTONESCU: I mean he's not on --

16 MEMBER SHACK: I am on. I was muted.

17 (Laughter.)

18 CHAIRMAN BLEY: He's not, but I wanted to  
19 make sure he was here.

20 MEMBER SHACK: You missed my wonderful  
21 speech.

22 (Laughter.)

23 CHAIRMAN BLEY: I hope you recorded it.

24 (Laughter.)

25 But before we get to the members, I guess

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I also should ask about the folks on the line.

2 Can we open up the phone line for the  
3 people who are listening in? And I would ask if any  
4 of you would like to make a comment. We will have to  
5 wait just a minute for this.

6 And we never did have to get to a closed  
7 session. Maybe in another meeting later.

8 So we will wait just a minute for that.

9 As we are waiting, I am going to start at  
10 this end, Mario, when we come around to all the  
11 members.

12 MEMBER BONACA: I have been somewhat  
13 encouraged by --

14 CHAIRMAN BLEY: Well, give us a second for  
15 this.

16 MEMBER BONACA: Yes.

17 CHAIRMAN BLEY: Is it open (referring to  
18 the phone line)?

19 MEMBER STETKAR: Somebody on the other end  
20 of the line just say something.

21 CHAIRMAN BLEY: Maybe they are all gone.

22 MEMBER STETKAR: Anyone just say anything.

23 (Laughter.)

24 PARTICIPANT: This is Shane Flores from  
25 Southern Nuclear. I don't have any additional

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *comments.*

2 *CHAIRMAN BLEY: Okay. But there is*  
3 *somebody there. Thank you.*

4 *(Laughter.)*

5 *Okay. We will now come to the members.*

6 *Mario? I'm sorry.*

7 *And both general comments on today, but*  
8 *also, if you are so inclined, your ideas of where we*  
9 *should go next or what we would like to hear next from*  
10 *the staff in this area.*

11 *MEMBER BONACA: My sense is that we saw an*  
12 *attempt to bridge the gap between us and the staff,*  
13 *and I think it was valuable. I still believe there is*  
14 *too much reliance on the inspectors' capability and on*  
15 *human elements to review and depend on that for the*  
16 *review that provides us with reasonable assurance. We*  
17 *are all human, and I think that I need to have a*  
18 *demonstration that this approach is going to work.*

19 *CHAIRMAN BLEY: Okay. Thanks.*

20 *Joy?*

21 *MEMBER REMPE: I think any comments that I*  
22 *would have would be similar, and that when you even go*  
23 *from one situation to another plant, that you might*  
24 *have some variability. I don't know how these types*  
25 *of situations will -- identifying new ITAAC or*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 something that wasn't totally adequate, I am not quite  
2 sure how those types of issues would be resolved.

3 CHAIRMAN BLEY: Okay. Mr. Brown?

4 MEMBER BROWN: I am just still trying  
5 to -- I mean it was a useful discussion, okay? So I  
6 appreciated the fact that the staff developed these  
7 examples and tried to give us a perspective on what  
8 they did. So I thought that was useful to let us hear  
9 that.

10 I am still trying to work my way through  
11 the idea of the separation between inspection and  
12 review or process-type-oriented stuff as being a  
13 potential substitute for design review-type, in  
14 certain areas, not across the board because I am not  
15 speaking of 100 percent design review or anything like  
16 that, but to certain critical attributes that we  
17 depend on for the overall framework, you know, above  
18 the clouds, up in the clouds, not down -- yes, above  
19 the clouds, not down in all the weeds, which I have  
20 articulated before, and that they are addressed from a  
21 design review standpoint once we get an actual design.

22 Process is obviously very important. You  
23 have got to have that to make sure you take care of  
24 all the standard stuff that is called out and all the  
25 various standards, but it doesn't set you apart from

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 doing a level of detailed design review in specific  
2 areas to make sure you meet the basic fundamentals of  
3 independence and redundancy, and all the other stuff  
4 that I have iterated time and time again, because  
5 those vary depending on what the design looks like and  
6 how they are executed and implemented.

7 And with the level of block diagrams that  
8 exist in the Design Certification Documents, they are  
9 not real explicit. Some have a few more words; some  
10 have a few less. And therefore, in other words,  
11 independence many times is in the eyes of the  
12 beholder, as well as deterministic behavior is in the  
13 eyes of the beholder. So you need to do a very  
14 thorough review of those.

15 So the mix of process versus actual  
16 hardware, you know, software, architecture design  
17 review, is of real concern to me as to how much we get  
18 into that realm, and how it is reflected in the DAC.

19 Some of the stuff we saw in one of the  
20 projects amplified those where they actually defined  
21 what they thought were the major things on how their  
22 program, or not the program architecture, but the  
23 actual programming should be done, what functions and  
24 type things to ensure deterministic behavior.

25 They were articulated in their DAC, and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that was a positive thing. Others don't say anything  
2 at all. So I am looking to how we balance that out  
3 and come up with an acceptable solution overall.

4 That's it.

5 CHAIRMAN BLEY: Okay. Thank you.

6 Mike?

7 MEMBER RYAN: I will try to generalize  
8 what I think has been said, at least in part, by the  
9 summary comments and also during the meeting.

10 I thank everybody for their presentations.

11 I know you have put a lot of work into this and  
12 really worked hard today and this afternoon to have a  
13 good dialog with us. I appreciate that.

14 I think you have got a two-edged sword  
15 here. One is you have got a tremendous amount of  
16 experience in inspection that you are bringing to  
17 this, a tremendous amount of technical expertise that  
18 you are bringing to this, with an experience that is  
19 not exactly aligned with what you are now going to be  
20 looking at.

21 So, the experience is great, and we are  
22 going to rely on that experience. We all do that.  
23 But you have got to constantly remind yourself, I may  
24 not be applying it in exactly the right way to get  
25 exactly the result that I am used to getting.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           So I would think about that a little bit  
2 and, then, maybe challenge yourselves in some way, in  
3 a formal way, as you go through the review process,  
4 you know, doing your inspections, to stop somewhere  
5 along in that process and say, "How are we doing?  
6 Have we really done the right things? Are we missing  
7 anything? Is there anything that came to anybody's  
8 mind that we should have looked at that we didn't look  
9 at that's not in the plan?" And have some mechanism  
10 to deal with that of maybe, I don't want to say  
11 changing the plan, but updating the plan, adding  
12 detail, and things like that, to at least examine the  
13 question, because this is new.

14           I mean digital I&C is a new area in lots  
15 of ways. And you have got the talent to do it, but I  
16 think you have just got to kind get committed to the  
17 idea that you ought to maybe formalize some sort of a  
18 cycle through that thought process I outlined there  
19 just very briefly, to make sure you are comfortable  
20 that you are still on track as you march through.

21           I think if you do that, that might help  
22 address some of the detail points, then, that Charlie  
23 has raised and the comments that John Stetkar has  
24 raised. If you can deal with it in a formal way that  
25 is transparent to everybody involved, the licensee and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 *staff here and your critical reviewers that you are*  
2 *going to have involved, and to the Committee here, we*  
3 *will all learn from that process, if you can find a*  
4 *way to make that happen.*

5 *Thank you, Dennis.*

6 *CHAIRMAN BLEY: Thank you.*

7 *Said?*

8 *MEMBER ABDEL-KHALIK: Okay. My concern*  
9 *is, and has always been, related to post-COL DAC*  
10 *closure. Specifically, that the inspection process*  
11 *and procedures will provide reasonable assurance that*  
12 *the design meets not just the literal wording of the*  
13 *DAC, but all -- underline "all" -- the requirements on*  
14 *which the safety case had been made.*

15 *Our, meaning ACRS, review of the*  
16 *inspection procedures, while absolutely necessary, is*  
17 *not, in my view, sufficient. We need to be involved*  
18 *in the, quote, "inspection process".*

19 *That is the end of my comments.*

20 *CHAIRMAN BLEY: Thank you.*

21 *ME. Stetkar?*

22 *MEMBER STETKAR: I would echo, not to*  
23 *belabor things, I would echo some of the things that*  
24 *Charlie said and also what Mike Ryan said.*

25 *Quite honestly, I am really intrigued by*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the challenges of this process. I am really  
2 interested to see firsthand how it works. And I don't  
3 think we know how it is going to work until we  
4 actually do it, regardless of what people say about  
5 assurances.

6 My focus is to have some confidence that  
7 the process results in the type of, what I call a  
8 robust, integrated engineering review of the as-built  
9 design, to the same level of assurance that would have  
10 been provided if the design details were available at  
11 the design certification stage.

12 The process can result in that. The  
13 process might not result in that if the process is  
14 simply an inspection process that confirms adherence  
15 to a large number of very detailed, catalogued,  
16 generic, check-off-the-box-type criteria. That is not  
17 an engineering review.

18 I will stop there. I was going to give my  
19 standard example about how conformance of all of the  
20 specified design engineering criteria can still result  
21 in a design that is not very sane when examined from  
22 an integrated perspective. But I'm not going to do  
23 that again. You have all heard it.

24 (Laughter.)

25 CHAIRMAN BLEY: Sam?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   **MEMBER ARMIJO:**    Yes, I think the process  
2 *post-closure, post-COL closure of DAC is my biggest*  
3 *concern.    The process looks very thorough, very*  
4 *complete, when everything goes right.    But, most of*  
5 *the time, things don't almost go perfectly well, and*  
6 *it is when things don't work out, how you recover.*

7                    *I think there's risks, both regulatory*  
8 *risk and, having come from a commercial side of the*  
9 *industry, I think there is enormous business risk.*  
10 *That is not my role here.*

11                   *But I think the sooner the applicants put*  
12 *a lot of effort into completing these designs, the*  
13 *better.    And those that are closing them out in the*  
14 *DCD and COL I think will be in much better shape, and*  
15 *we will understand it a lot better.    We will have a*  
16 *role in the ACRS.    We will have a role in that.*

17                   *Not having any input in the initial post-*  
18 *COL closures seems to be a mistake.    I think that we*  
19 *made that point in our letter.*

20                    *So that is all I have.*

21                   **CHAIRMAN BLEY:**    Okay.    Thank you, Sam.

22                    *Bill?*

23                   **MEMBER SHACK:**    I was impressed by the  
24 *presentation.*

25                    *Oops, am I still on?*

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                    **CHAIRMAN BLEY:** Yes.

2                    **MEMBER SHACK:** Okay. My concern is  
3 somewhat like Mike's and John's, that we have  
4 relatively limited experience with these systems. At  
5 least that is my impression. You know, we have only  
6 approved a limited number of applications.

7                    So, with something like the FMEA, you  
8 know, in the DAC approach, you are going to have a  
9 relatively limited set of eyes looking at that final  
10 FMEA. Whereas, if we were doing it in the design  
11 review, you might have more perspective on it. So  
12 there is a certain limiting nature there. I think the  
13 process can work.

14                    One thing that might be interesting is to  
15 hear something about the results of the inspection at  
16 South Texas. I mean, although they are still at the  
17 high level, and it is not our concern, it still might  
18 be interesting to hear somebody's reflections on the  
19 experience.

20                    That's all.

21                    **CHAIRMAN BLEY:** Anything else?

22                    (No response.)

23                    Okay. And I guess I admit to being rather  
24 encouraged. I think we have moved a lot closer  
25 together than in the past, or if we haven't moved

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 closer together, where staff is headed with this is a  
2 lot more clearly defined.

3 We had a lot of trouble over the last  
4 several years trying to figure out just what this was  
5 going to look like. I know you are just in the midst  
6 of formalizing that. I think going through that  
7 process is really helpful and important, and will get  
8 us to something useful.

9 The level of detail in the inspections and  
10 audits that you went through today has explained that  
11 process better than I have heard in the meetings with  
12 the Design Centers. So I am a little encouraged by  
13 that as well. And I think more of these sessions will  
14 be helpful. Now hearing what is happening at South  
15 Texas will be crucial to this going forward.

16 I do understand -- is Gerry still here? --  
17 I do understand Gerry Wilson's point about the  
18 hesitancy of bringing Tier 2 into Tier 1 because that  
19 makes it Tier 1. But something like what you showed  
20 us from ESBWR, or maybe something even more specific  
21 than that on particular points, some kind of cross-  
22 referencing matrix, can get us to perhaps the same  
23 point. So something along that line would be helpful.

24 And there, I expect one day we will start  
25 hearing about guidance for the next design reviews

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that would incorporate that and how they would be  
2 done, and get us somewhat closer.

3 The one thing we didn't talk about much is  
4 the concern by some of our members, and I think by  
5 staff as well from discussions we have had, is once  
6 this goes post-COL, it is possible to polarize and  
7 come down to what is the letter of what is in the  
8 documentation.

9 The point that it is understood that all  
10 these other pieces are linked together and have to be  
11 met is one that may well be true, but it seems like  
12 one that could be challenged, if somebody chose to  
13 challenge it. I have a little trouble anticipating  
14 that happening because nobody wants a system that is  
15 not going to protect the plant.

16 So, anyway, I think we have gotten a lot  
17 from this, and I want to thank the staff for some good  
18 presentations and discussions.

19 It looks like ME. Stetkar wants to say  
20 something more.

21 **MEMBER STETKAR:** Just to make a point.  
22 You emphasized the detail in the cross-referencing and  
23 indexing that we saw today. Those are Tier 2  
24 information. That is not --

25 **CHAIRMAN BLEY:** Yes.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   MEMBER STETKAR:    Okay.    So that doesn't  
2 necessarily --

3                   CHAIRMAN BLEY:    But it is not written into  
4 Tier 1 and it is sections rather than details.

5                   MEMBER STETKAR:    That's right.

6                   CHAIRMAN BLEY:    Yes.

7                   MEMBER BROWN:    If I can amplify one other  
8 point that you made?

9                   CHAIRMAN BLEY:    Yes.

10                  MEMBER BROWN:    ESBWR did add a huge number  
11 of DAC listings and line items, as well as a  
12 considerable additional discussion, 23 pages worth or  
13 something like that, expanding on their discussions to  
14 more fully explain what they were doing.  And that's  
15 Tier 2, but the DAC was Tier 1.

16                  CHAIRMAN BLEY:    And I guess one last point  
17 from me.  We didn't have this meeting to talk about  
18 your response to our letter, but there are at least  
19 two points -- and I am not speaking for the Committee  
20 here -- there are at least two points where it seems  
21 we are not quite on the same page.

22                                The one is we are still saying that it  
23 would be really nice to limit DAC as much as possible.

24                                And it seems that that wasn't emphasized.  In other  
25 documents from staff, there seems to be not a concern

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 about the numbers of DAC or the extent of DAC. We  
2 think the idea of limiting it as much as possible is  
3 important for future plants.

4 And I guess the other one is the ACRS  
5 involvement. The argument is made that the  
6 involvement of ACRS in inspections for DAC is  
7 analogous to the inspections in Part 50. And at least  
8 I think that is somewhat, not somewhat, quite a bit  
9 different, in that in Part 50 you didn't get the  
10 operating license until the design was complete. So  
11 there is a fuzziness there that I think still is a  
12 matter of difference.

13 Nothing else?

14 I'm sorry. Yes, Dan, go ahead, and then  
15 back to Laura.

16 ME. SANTOS: On your first point, we will  
17 provide you with that table. In digital I&C the use  
18 of DAC is dramatically declining. It is declining.  
19 The use is declining. AP1000, one; USAPR, maybe two,  
20 USAPWR, none. So we will provide you with that table.

21 MEMBER STETKAR: And ESBWR you didn't  
22 mention.

23 ME. SANTOS: Hundreds.

24 MEMBER STETKAR: Hundreds? Okay. Thanks.

25 (Laughter.)

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1                   CHAIRMAN BLEY: Anything more?

2                   ME. SANTOS: And the other point, the due  
3 time, through Christina, if you could inform us what  
4 is the next step with the Subcommittee to continue the  
5 dialog on moving us forward?

6                   CHAIRMAN BLEY: Okay.

7                   ME. SANTOS: So for us to understand from  
8 the staff what are the next steps.

9                   MS. DUDES: Okay. Thanks, Dan.

10                   Yes, again, I think we are going to  
11 capture that. I just appreciate the opportunity, and  
12 I appreciate the comments.

13                   I am hoping that when we talked about what  
14 we wanted to accomplish, that you see that the staff  
15 is very confident in their safety findings in the DCD  
16 and the rigor and the depth that they go to, and how  
17 they relate the DAC and ITAAC.

18                   One of the things that I hope we were able  
19 to express that we also have, I am not going to say --  
20 we are taking a very measured approach. We understand  
21 this is a first-time implementation. So, as we are  
22 working as a team to develop the inspection  
23 procedures, to do the pilot inspection, to get your  
24 review and advice on those procedures.

25                   And we actually have it as an action, and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we would have done it anyway, to come and brief you on  
2 the results of the STP pilot because I think the more  
3 eyes that we have on these initial activities, the  
4 better we can implement them in the future.

5 And it goes along to what you were saying.

6 Staff is very focused, as we take these next steps,  
7 into getting to final closure documents on both the  
8 DAC and the ITAAC, in not missing issues, and in  
9 having a continual feedback loop in our process to  
10 say: here's the procedure. Here's what we found.  
11 How is it working out with the inspectors? How are  
12 the procedures being used by the inspectors? How are  
13 they able to map back to the DCD?

14 So I hope that we have made it clear that  
15 we don't think that these tasks (a) are simple. I  
16 think someone said, well, yes, it could be successful.

17 I mean I think we are very skeptical, taking our time  
18 and moving very slowly on that. So I think that,  
19 hopefully, we expressed that to you, that we plan to  
20 take measured steps and use feedback and lessons  
21 learned on this issue.

22 I think that is all that I have to say. I  
23 think you characterized some of the issues that still  
24 remain and some of the concerns. I think we will need  
25 to just continue to work together.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I know the full Committee will be getting  
2 together, and that is a good time when we can talk  
3 about the response and if you have more specific  
4 issues.

5 One of the challenges, I will say, you  
6 know, we talk about the Design Center meeting, and you  
7 can come up with -- there's thousands of pages over  
8 there. You can come up with a question on almost  
9 anything. And sometimes we can really go down the  
10 rabbit hole.

11 I would like us to prepare as much as  
12 possible so that we are focused and maybe taking the  
13 smaller chunks, so that when you have questions, we  
14 are able to answer them on the spot and direct them,  
15 or if we can't answer them, get back to you, as  
16 opposed to lecture about why we can't answer them.

17 But, you know, it has been a long  
18 afternoon, but I think very worthwhile. I learned  
19 quite a bit, and I truly appreciate your time.

20 CHAIRMAN BLEY: Well, thanks to everyone.

21 And this meeting is adjourned.

22 (Whereupon, at 5:40 p.m., the proceedings  
23 in the above-entitled matter were adjourned.)

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



# Design Acceptance Criteria for New Reactors

Laura Dudes

Daniel J. Santos

Division of Engineering, Office of New Reactors

October 21, 2010

# Purpose

- Seek feedback from the ACRS to help arrive at a common understanding of concerns associated with resolution of DAC.
- Present the method used by staff to arrive at a safety finding.
- Present the method used by staff to resolve DAC.

# Expected Outcomes

- Common understanding of ACRS concerns.
- Common understanding of staff's review and safety finding.

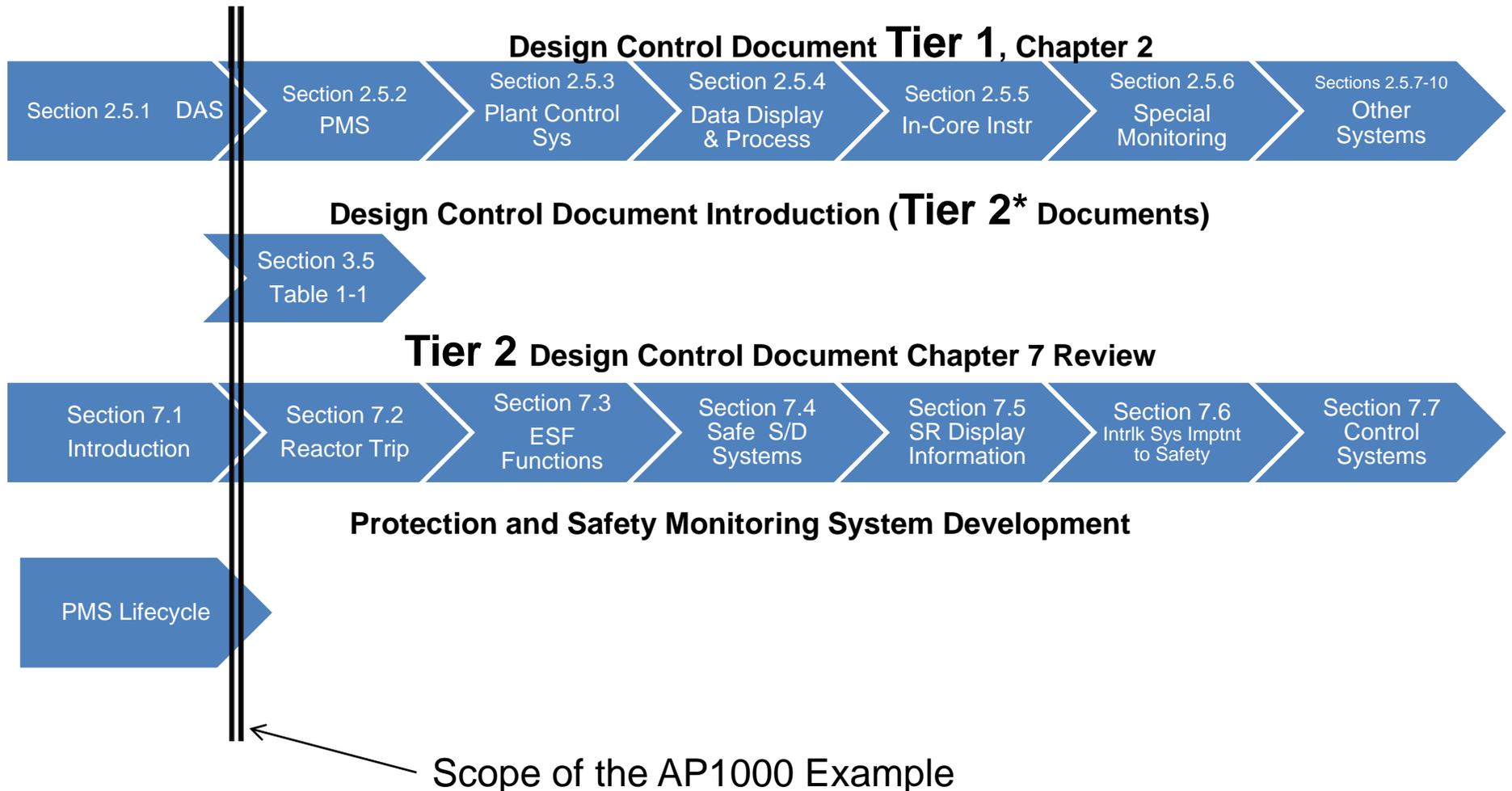
# Recent Developments

- ACRS letter August 9, 2010
  - Recommendations
  - Additional concerns
- AP1000, ESBWR, Digital I&C subcommittee meetings in September 2010
  - Depth of DI&C reviews in the DAC/ITAAC process
- Staff response to ACRS letter issued on October 7, 2010
  - Staff agrees that resolution of DAC requires expert judgment
  - ACRS role in inspection program development

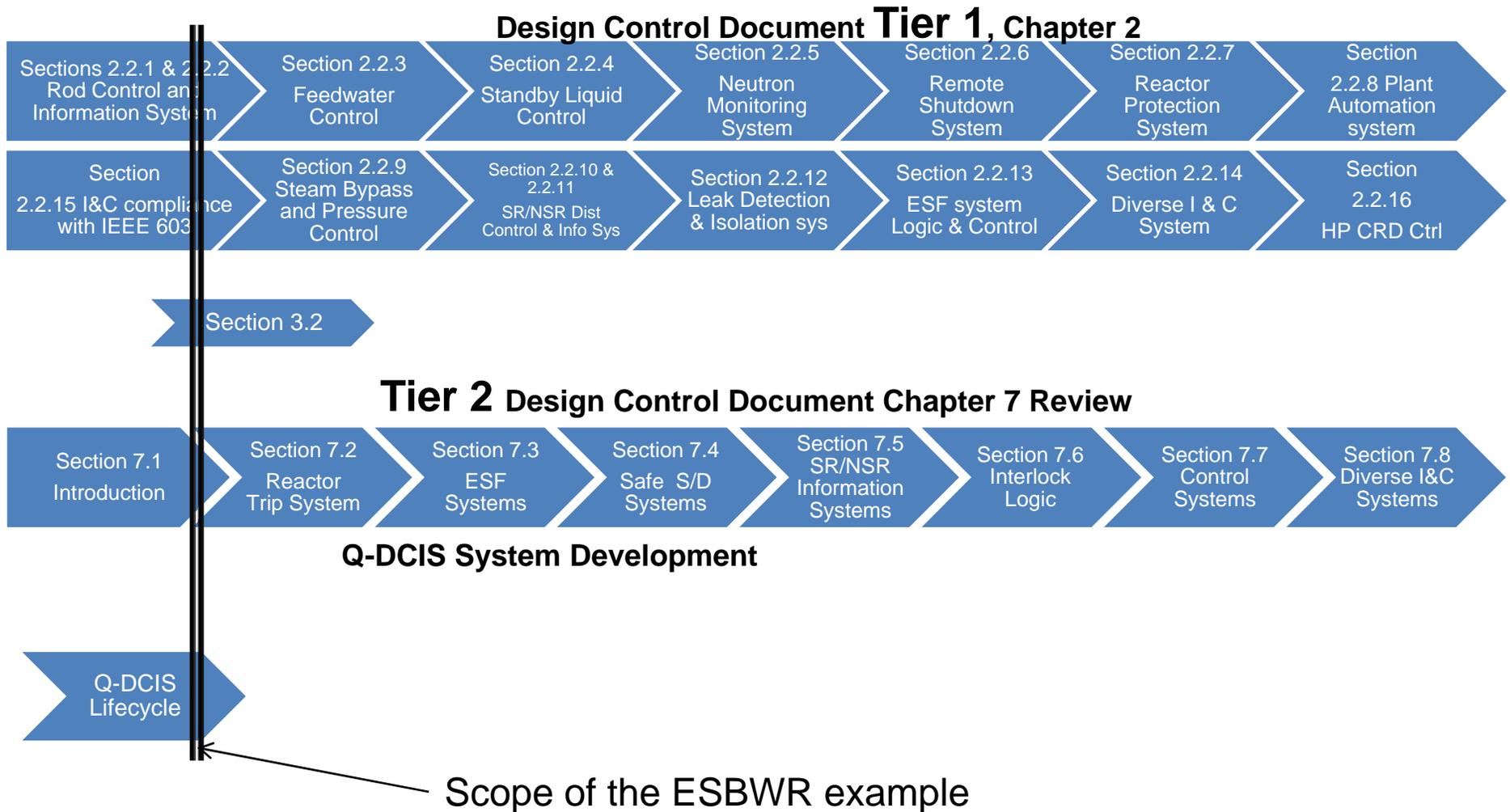
# Two Examples

- AP1000
  - PMS development process
  - Being resolved by the applicant (WEC) through Design Certification process (amendment)
- ESBWR
  - Single Failure Criteria
  - To be resolved after license is issued by COL holder

# Vertical Cross Section of DAC Review Process Related to IV&V



# Vertical Cross Section of DAC Review Process Related to Single Failure Criterion



# Presentation Outline

- DAC resolution method, scope, and depth of evaluation
  - Describe the safety issue, safety significance, safety finding.
  - Describe the associated regulatory requirements to satisfy the safety issue.
  - Summary and relevant examples of information submitted by the applicant including an analysis of the proposal in terms of regulatory requirements, established staff positions, industry standards, or other relevant criteria.
  - A brief explanation of the method used by the staff for its review.
  - Explanation by the staff as to why it was acceptable to have this particular DAC.
  - Staff assessment of the quality of the DAC itself.
  - How will the DAC be resolved? Roles and responsibilities (who does what, when and with what?)

# BACKUP SLIDES

# Licensing and Design Documents within and beyond FSAR

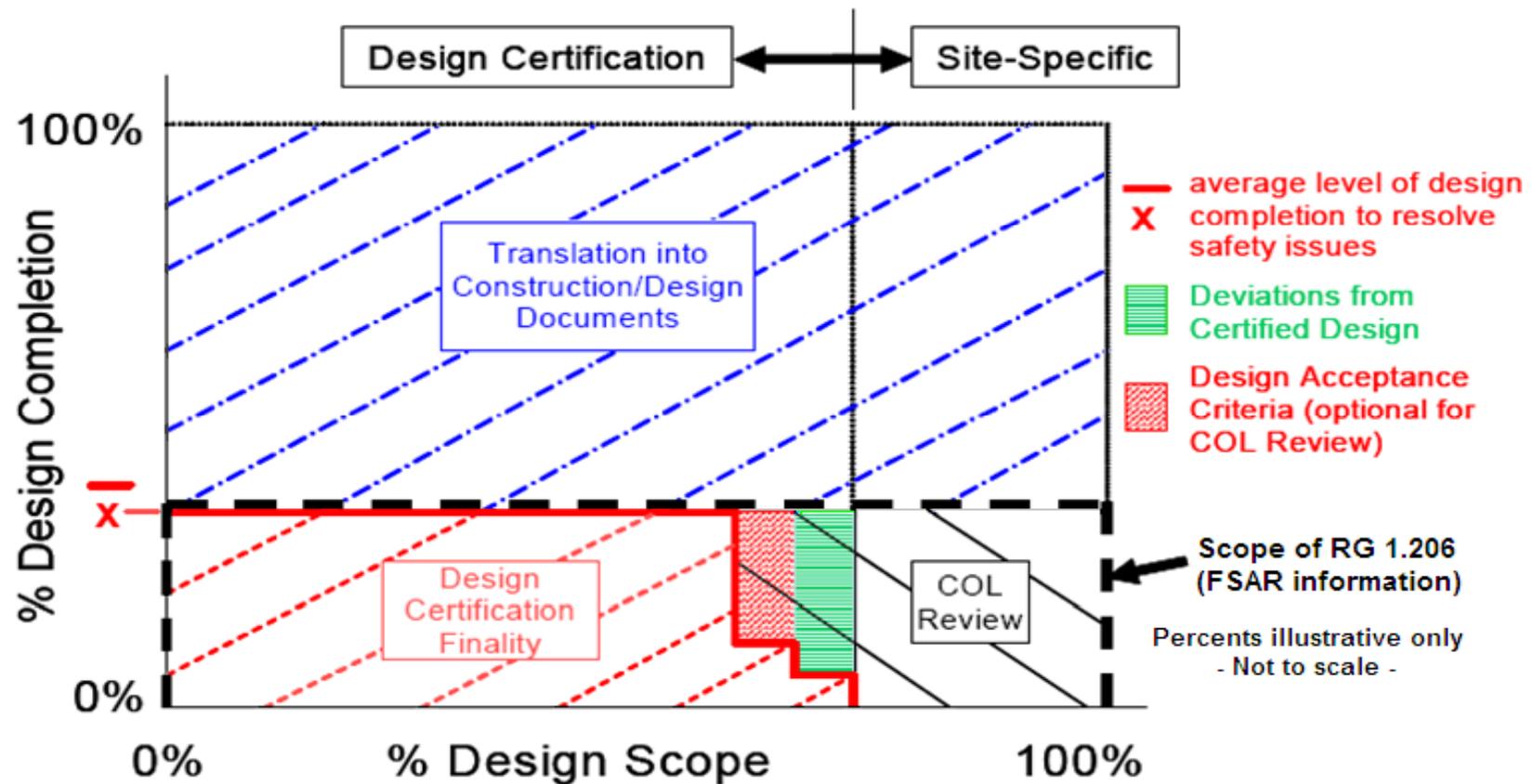
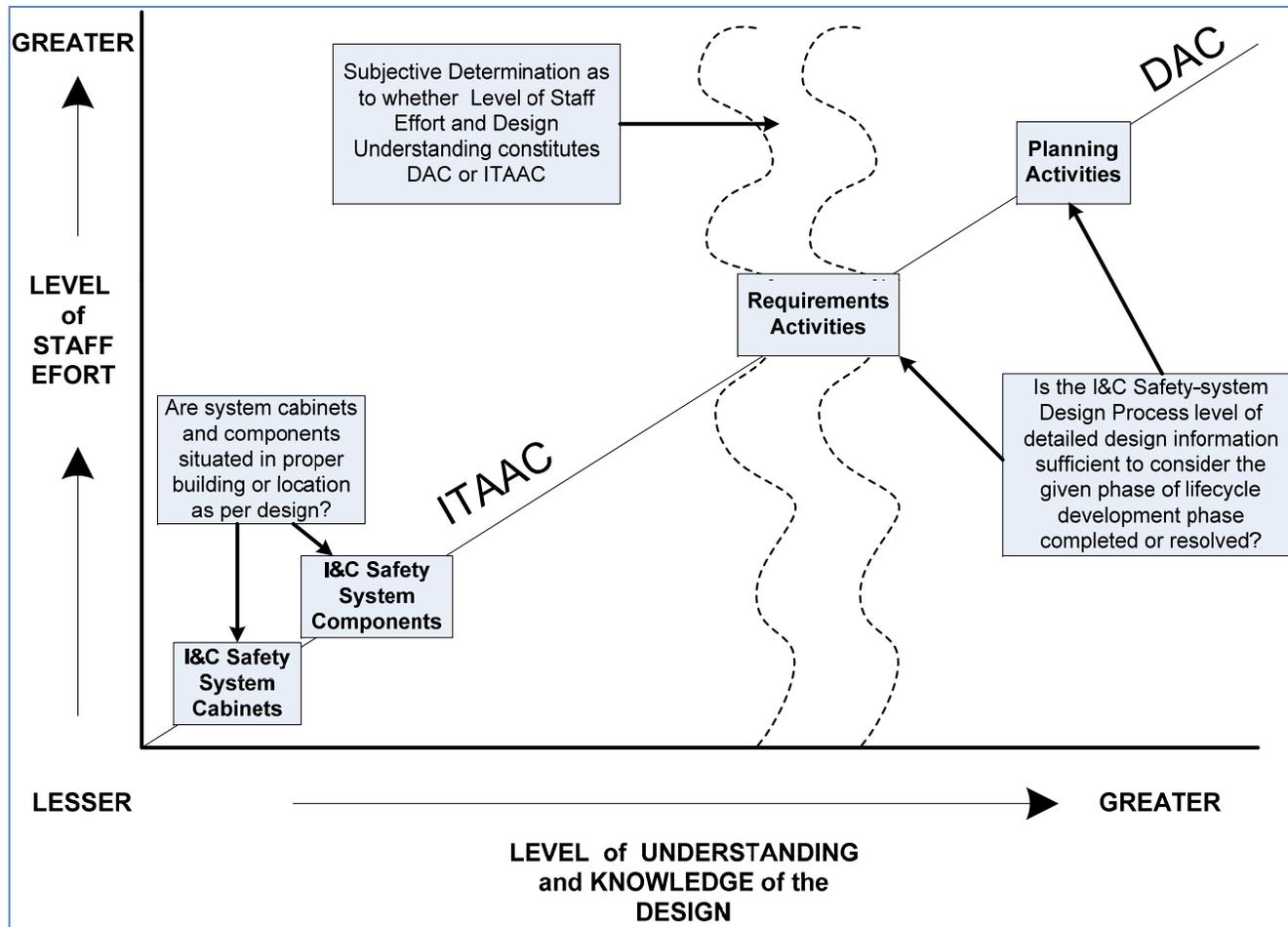


Figure 1 (from RG 1.206, Section B, “Discussion”): Combined License Referencing a Certified Design

# DAC/ITAAC Level of Effort and Design Understanding Graph





# Resolution Process for AP1000 Instrumentation and Controls Design Acceptance Criteria

Terry Jackson  
William Roggenbrodt

Instrumentation, Controls, and Electrical Engineering Branch 1  
Division of Engineering  
**October 21, 2010**

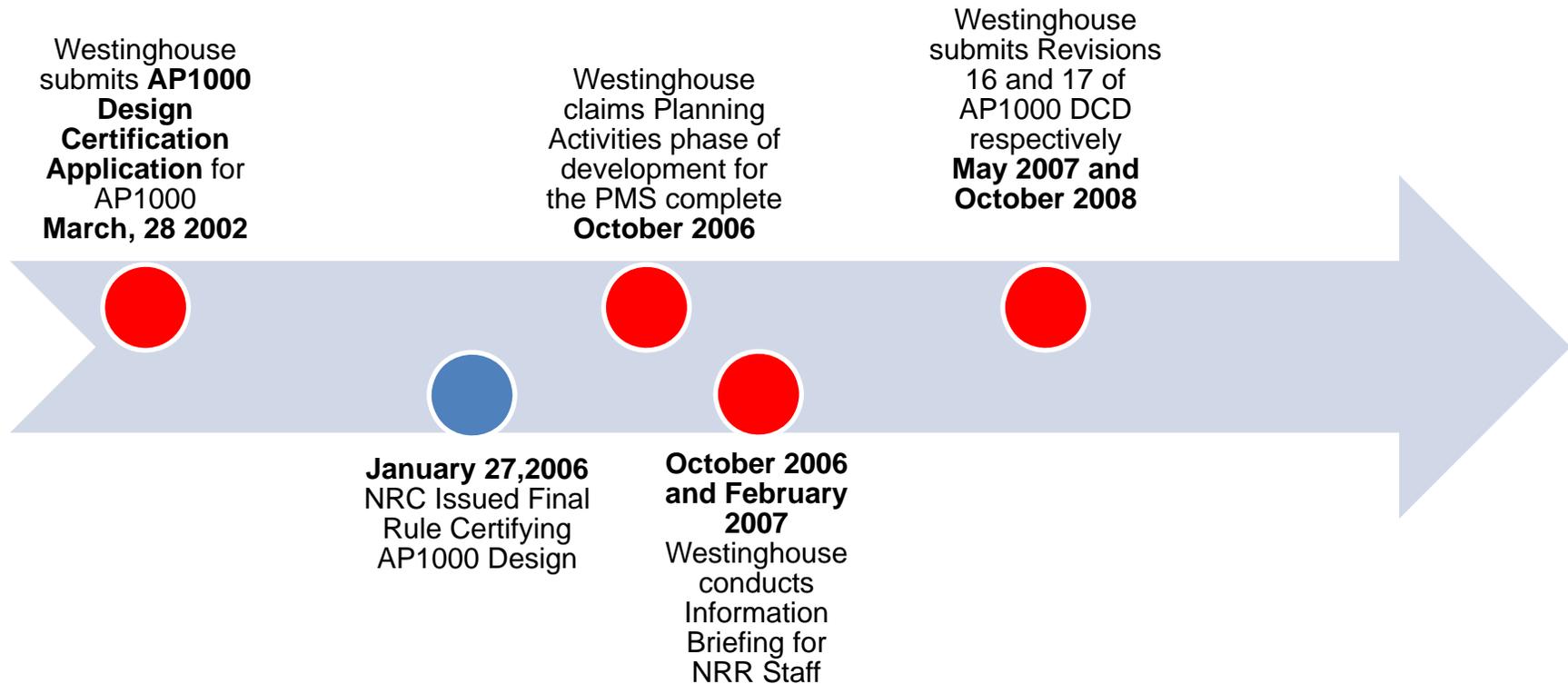
# Purpose

- Demonstrate the level of effort and depth of review the staff uses to resolve Design Acceptance Criteria (DAC) through an AP1000 example.
- Identify the requirements, guidance, documents, and resources used to resolve DAC.
- Correlate the staff efforts used in this example to future DAC resolution.
- Anticipated Outcome: Better understanding of the scope of staff effort and review for DAC resolution and the tools and resources used.

# Outline

- AP1000 Timeline
- AP1000 DAC Example
  - Safety Issue and Significance
  - Regulatory Requirements and Criteria
  - AP1000 Licensing Basis Listed in Tier 1 and 2
  - Staff's Safety Finding Regarding DAC
  - Staff's Activities to Address Resolution of DAC
  - Current Status of AP1000 DAC
- Future Activities to Address DAC

# AP1000 Timeline (2002 – 2008)



**NOTE: Relative distance on timeline not drawn to scale**

# AP1000 DAS DAC/ITAAC

## Item 4 of Tier 1, Table 2.5.1-4 (cont.) Inspections, Tests, Analyses, and Acceptance Criteria (Revision 15 of the DCD shown)

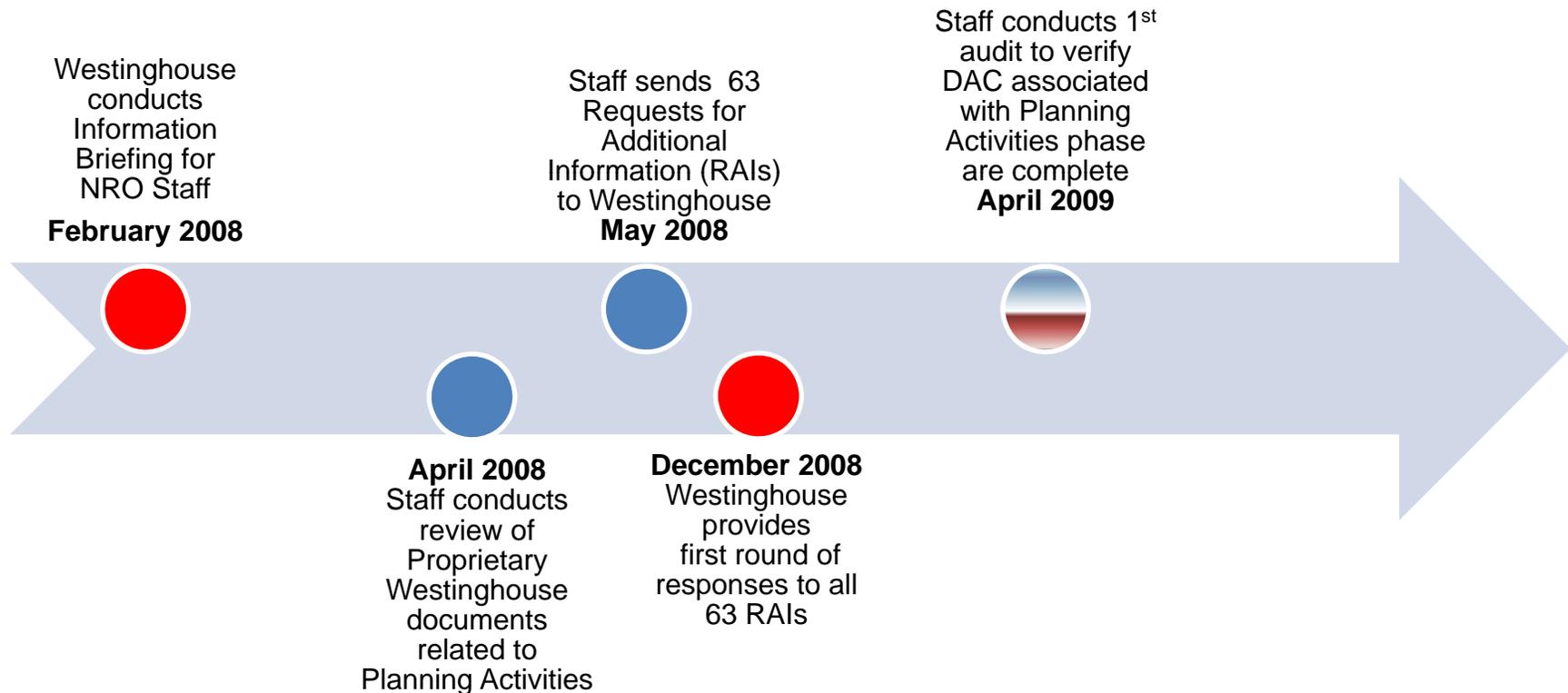
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
<p>4. The DAS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:</p> <ul style="list-style-type: none"> <li>a) <b>Design requirements phase</b></li> <li>b) <b>System definition phase</b></li> <li>c) Hardware and software development phase</li> <li>d) System test phase</li> <li>e) Installation phase</li> </ul>	<p>Inspection will be performed of the process used to design the hardware and software.</p>	<p>A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following:</p> <ul style="list-style-type: none"> <li>a) <b>Establishment of plans and methodologies during DR phase.</b></li> <li>b) <b>Specification of functional requirements during the SD phase</b></li> <li>c) Documentation and review of H/W and S/W during the H/W and S/W development phase.</li> <li>d) Performance of system tests and the documentation of system test results during ST phase.</li> <li>e) Performance of installation tests and inspections during install phase.</li> </ul>

# AP1000 PMS DAC/ITAAC

## Item 11 of Tier 1, Table 2.5.2-8 (cont.) Inspections, Tests, Analyses, and Acceptance Criteria (Revision 15 of the DCD shown)

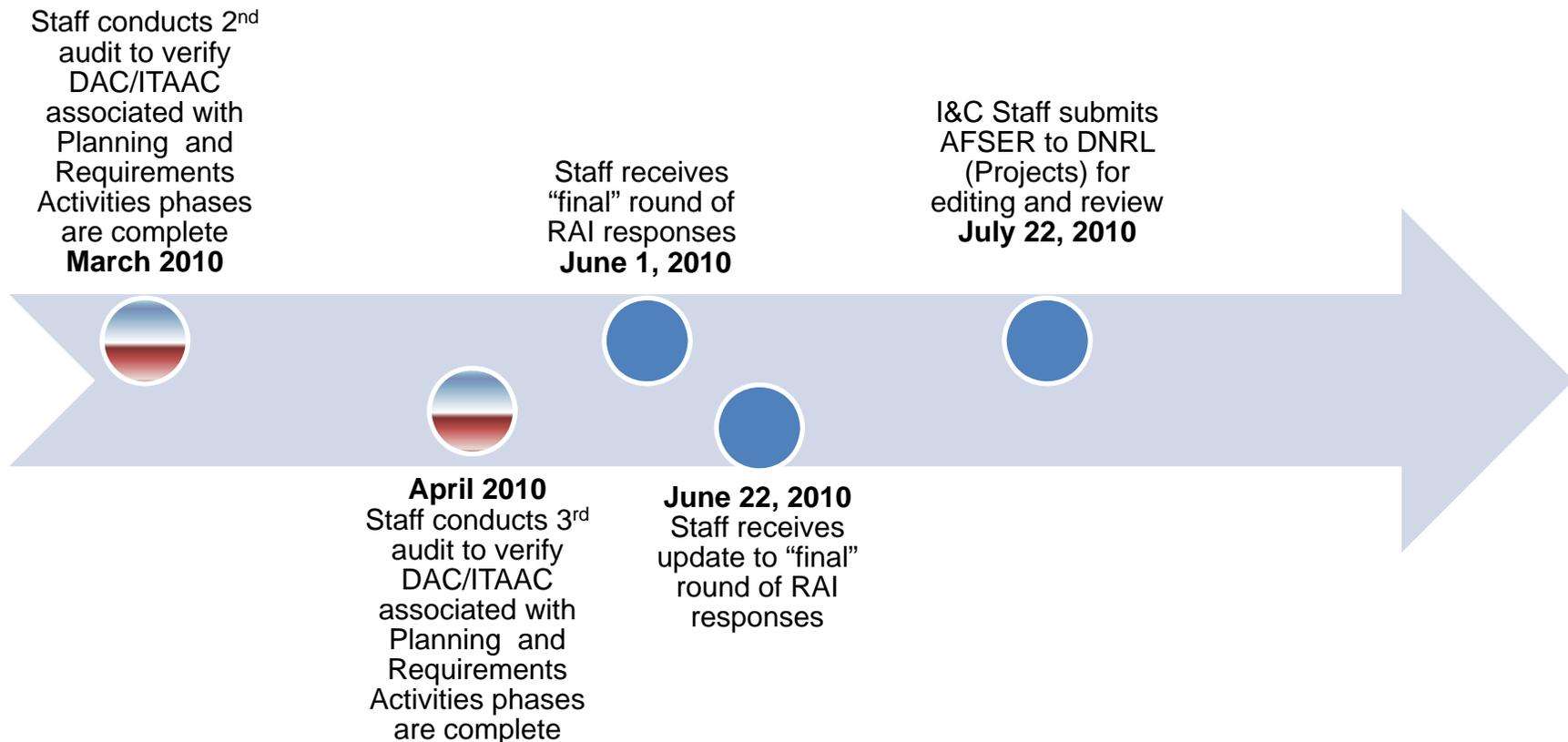
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
<p>11. The PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:</p> <ul style="list-style-type: none"> <li><b>a) Design requirements phase, may be referred to as conceptual or project definition phase</b></li> <li><b>b) System definition phase</b></li> <li>c) Hardware and software development phase, consisting of hardware and software design and implementation</li> <li>d) System integration and test phase</li> <li>e) Installation phase</li> </ul>	<p>Inspection will be performed of the process used to design the hardware and software.</p>	<p>A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following:</p> <ul style="list-style-type: none"> <li><b>a) Establishment of plans and methodologies.</b></li> <li><b>b) Specification of functional requirements.</b></li> <li>c) Documentation and review of hardware and software.</li> <li>d) Performance of system tests and the documentation of system test results.</li> <li>e) Performance of installation tests and inspections.</li> </ul>

# AP1000 Timeline (2008 – 2009)



**NOTE: Relative distance on timeline not drawn to scale**

# AP1000 Timeline (2010)



**NOTE: Relative distance on timeline not drawn to scale**

# AP1000 Tier 1 Design Description for DAS Lifecycle Development Process

AP1000 DCD, Tier 1, Chapter 2, Section 2.5.1 DAS

REVISION 15 of DCD	REVISION 16 of DCD	REVISION 17 of DCD
<p><b>Design Description 4</b> The DAS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:</p>	<p><b>Design Description 4</b> The DAS hardware and <u>any</u> software <del>is</del><u>are</u> developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:</p>	<p><b>Design Description 4</b> The DAS hardware and any software are developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:</p>
<ul style="list-style-type: none"> <li>a.) Design Requirements phase</li> <li>b.) System Definition phase</li> <li>c.) H/W and S/W Development Phase</li> <li>d.) System Test Phase</li> <li>e.) Installation Phase</li> </ul>	<ul style="list-style-type: none"> <li>a.) Design Requirements phase</li> <li>b.) System Definition phase</li> <li>c.) <del>H/W and S/W</del> Development Phase <u>for H/W and any S/W.</u></li> <li>d.) System Test Phase</li> <li>e.) Installation Phase</li> </ul>	<ul style="list-style-type: none"> <li>a.) Development Phase for H/W and any S/W.</li> <li>b.) System Test Phase</li> <li>c.) Installation Phase</li> </ul>

# AP1000 Tier 1 Design Description for PMS Lifecycle Development Process

AP1000 DCD, Tier 1, Chapter 2, Section 2.5.2 PMS

REVISION 15 of DCD	REVISION 16 of DCD	REVISION 17 of DCD
<p><b>Design Description 11</b> The PMS hardware (H/W) and software (S/W) is developed using a planned design process which provides for specific design documentation and reviews during the following lifecycle stages</p>	<p><b>Design Description 11</b> The PMS hardware (H/W) and software (S/W) is developed using a planned design process which provides for specific design documentation and reviews during the following lifecycle stages</p>	<p><b>Design Description 11</b> The PMS hardware (H/W) and software (S/W) is developed using a planned design process which provides for specific design documentation and reviews during the following lifecycle stages</p>
<ul style="list-style-type: none"> <li>a.) Design Requirements</li> <li>b.) System Definition</li> <li>c.) H/W and S/W Development Phase, Consisting of H/W and S/W Design and Implementation</li> <li>d.) System Integration &amp; Test</li> <li>e.) Installation</li> </ul>	<ul style="list-style-type: none"> <li>a.) System Definition</li> <li>b) H/W and S/W Development Phase, Consisting of H/W and S/W Design and Implementation</li> <li>c.) System Integration &amp; Test</li> <li>d.) Installation</li> </ul>	<ul style="list-style-type: none"> <li>a.) H/W and S/W Development Phase, Consisting of H/W and S/W Design and Implementation</li> <li>b.) System Integration &amp; Test</li> <li>c.) Installation</li> </ul>

# AP1000 Tier 1 DAC/ITAAC for DAS Lifecycle Development Process

AP1000 DCD, Tier 1, Chapter 2, Section 2.5.1 DAS, Table 2.5.1-4

REVISION 15 of DCD			REVISION 16 of DCD			REVISION 17 of DCD		
Design Commitment 4	ITA	A C	Design Commitment 4	ITA	A C	Design Commitment 4	ITA	A C
a.) Design Requirements			Design Requirements			<del>Design Requirements</del>		
b.) System Definition			a.) System Definition			<del>System Definition</del>		
c.) H/W and S/W Development			b.) Development Phase for H/W and any S/W			a.) Development Phase for H/W and any S/W		
d.) System Test			c.) System Test			b.) System Test		
e.) Installation			d.) Installation			c.) Installation		

# AP1000 Tier 1 DAC/ITAAC for PMS Lifecycle Development Process

AP1000 DCD, Tier 1, Chapter 2, Section 2.5.2 PMS, Table 2.5.2-8

REVISION 15 of DCD			REVISION 16 of DCD			REVISION 17 of DCD		
Design Commitment 11	ITA	A C	Design Commitment 11	ITA	A C	Design Commitment 11	ITA	A C
a.) Design Requirements			<del>Design Requirements</del>			<del>Design Requirements</del>		
b.) System Definition			a.) System Definition			<del>System Definition</del>		
c.) H/W and S/W Development & Implementation			b.) H/W and S/W Development & Implementation			a.) H/W and S/W Development & Implementation		
d.) System Integration & Test			c.) System Integration & Test			b.) System Integration & Test		
e.) Installation			d.) Installation			c.) Installation		

# AP1000 PMS

## Design Requirements DAC

- Safety Significance of PMS
  - Performs reactor trip, engineered safety features actuation, and qualified data processing (Post-Accident Monitoring) functions.
- Safety Significance of PMS Design Requirements (Planning) Lifecycle Phase
  - Identifies the high quality process by which PMS hardware and software are designed, fabricated, installed, and tested.
  - First step to ensure quality assurance.

# AP1000 PMS DAC

## Regulatory Requirements

- These are the specific requirements to AP1000 PMS Design Requirements Phase:
  - 10 CFR 50.55a(a)(1)
  - 10 CFR 50.55a(h)
    - IEEE Standard (Std.) 603 – 1991, Clause 5.3
  - 10 CFR Part 50 Appendix A, General Design Criteria (GDC)
    - GDC 1
  - 10 CFR Part 50 Appendix B
    - Criterion III
- The staff found that the AP1000 complied with these requirements in the certified design and the amendment.

The next question is...

Against what acceptance criteria did the staff evaluate the applicant's submittals?

# AP1000 PMS DAC Licensing Basis

- Westinghouse committed to follow the guidance contained in regulatory guides related to the software life cycle development process.

AP1000 DCD, Tier 2, Chapter 1, Appendix 1A, Pages 1A-63 to 1A-64, Revision 17  
REGULATORY GUIDE/DCD SECTION CROSS-REFERENCES

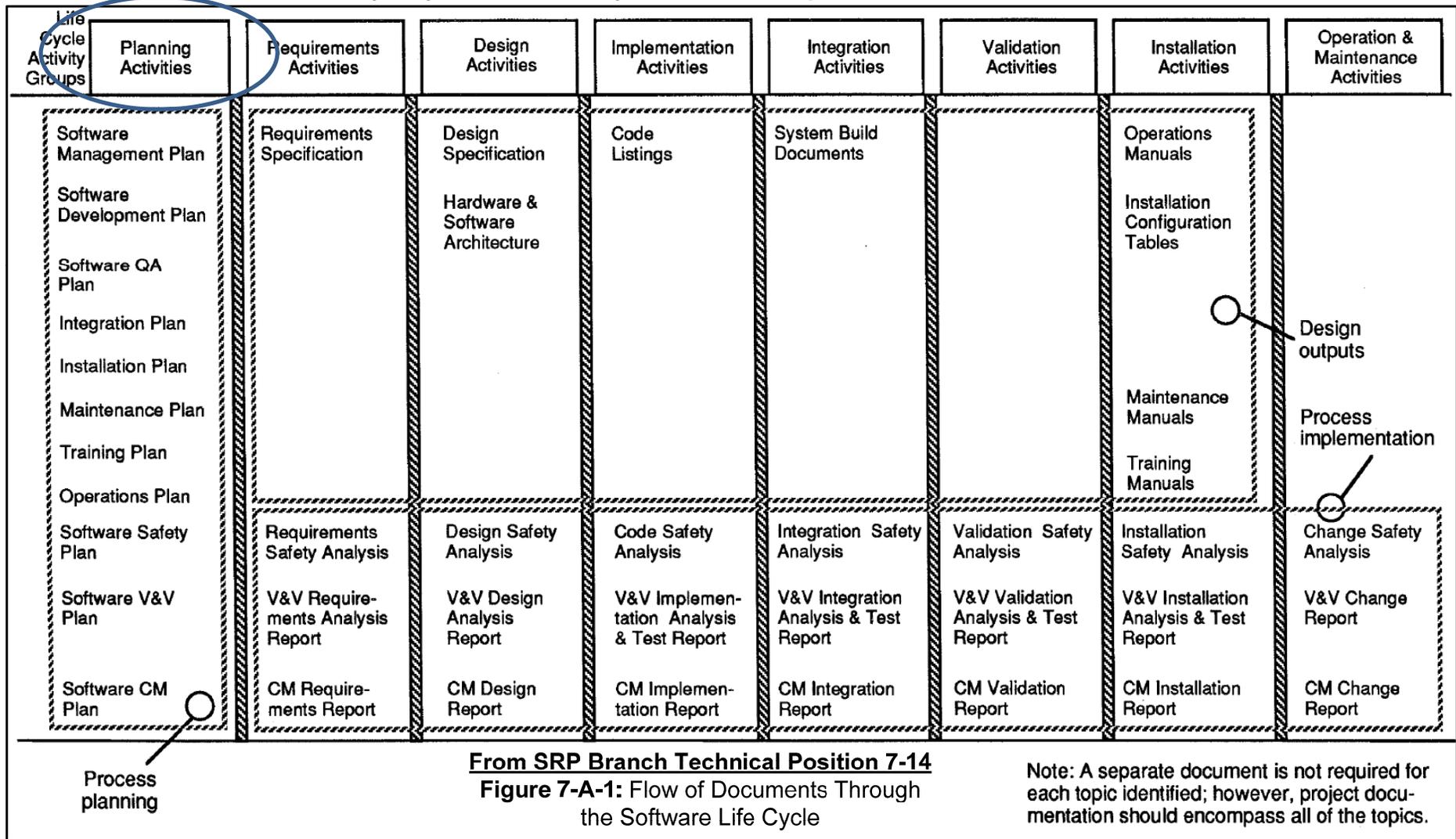
Division 1 Regulatory Guide		Commitment
1.152	Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants (Task 1C 127-5) (Rev. 1, January 1996)	Conforms
1.168	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 0, September 1997)	Conforms
1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 0, September 1997)	Conforms
1.170.	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 0, September 1997)	Conforms
1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 0, September 1997)	Conforms
1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 0, September 1997)	Conforms
1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 0, September 1997)	Conforms

# AP1000 PMS DAC Licensing Basis

- NUREG 0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition (SRP), Chapters 7 and 14
  - Branch Technical Position HICB – 14 – Guidance on S/W reviews for Digital Computer-Based I&C Systems
  - Commitment identified in AP1000 DCD, Tier 2, Section 1.9.2 via WCAP-15799, “AP1000 Compliance to SRP Acceptance Criteria,” Revision 1, Page 7-7 (ADAMS ML032541010)
- WCAP-16096-NP-A, “Software Program Manual for Common Q Systems,” Revision 1 (Identified as Tier 2\*)
- WCAP-15927, “Design Process for AP1000 Common Q Safety Systems,” Revision 2 (Identified as Tier 2\*)

# PMS DAC Review Process

I&C Safety System Lifecycle Development Process HICB 7-14



# AP1000 PMS DAC Staff Acceptance

- In 2006, in Section 7.1.4 of NUREG-1793, the AP1000 FSER, the staff accepted the use of DAC for the certified design (Revision 15) since the PMS was characterized as rapidly changing technology as discussed in SECY-02-0059, “Use of Design Acceptance Criteria for the AP1000 Standard Plant Design.”
- Design commitments in the AP1000 Tier 1 and Tier 2 DCD, as well as the DAC/ITAAC provide those procedures and attributes necessary for the staff to reach a reasonable assurance of safety finding.

# AP1000 Amendment DAC Review Process

- For the proposed AP1000 amendment, in addition to the DCD, staff evaluated 29 Westinghouse documents related to the PMS Planning and Requirements Activities phases of development. These documents were docketed.
  - WCAP-16097-P-A Common Qualified Platform Topical Report (3)
  - WCAP-16096-NP-1A Software Program Manual for Common Q Systems (2)
  - WCAP-15927 AP1000 Common Q Design Process (3)
  - WCAP-15776 Safety Criteria for AP1000 I&C Systems (1)
  - WCAP-16361-P PMS Setpoint Methodology (1)
  - WCAP-16675-P PMS Architecture (3)
  - WCAP-16674-P Data Communications and Manual Control (3)
  - WCAP-17179-P CIM Technical Report (3)
  - WCAP-17201-P PMS Compliance W/Selected ISGs (1)
  - WCAP-17226-P In-core Instrumentation System / PMS Separation Criteria (3)
  - WCAP-16438-P AP1000 Failure Modes and Effects Analysis (2)
  - WCAP-16592-P AP1000 Software Hazards Analysis (2)
  - APP-GW-J0R-012 Computer Security (2)

( ) the number in the Parenthetical relates to the number of revisions the report underwent prior to its acceptance by the staff

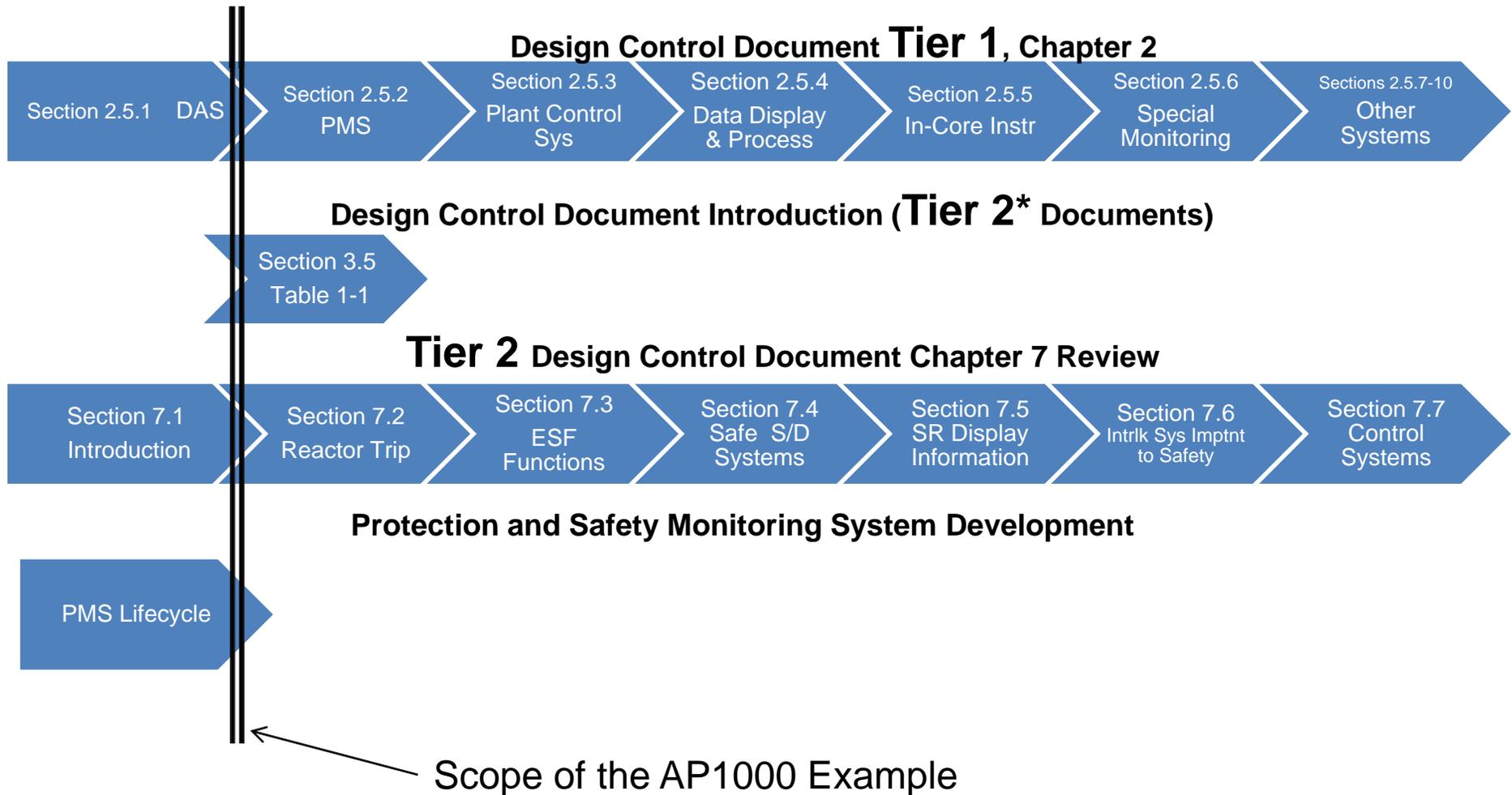
# AP1000 DAC Review Process

- Staff evaluated over 100 WEC proprietary documents related to the Design Requirements and System Definition phases of DAS and PMS development.
- Staff conducted three audits related to the two DAS and PMS development phases.
- Review and audit teams consisted of staff members from I&C, human factors engineering, technical specifications, probabilistic risk assessment, and system performance branches, as well as Region II staff.
- **In the 3 ½ years since the Office of New Reactors inception there have been:**
  - **5,224** Man-hours worked on the AP1000 DCA review
  - **113** Requests for Additional Information presented to WEC and
  - Over **6,160** pages of docketed information reviewed

# AP1000 DAC Review Process

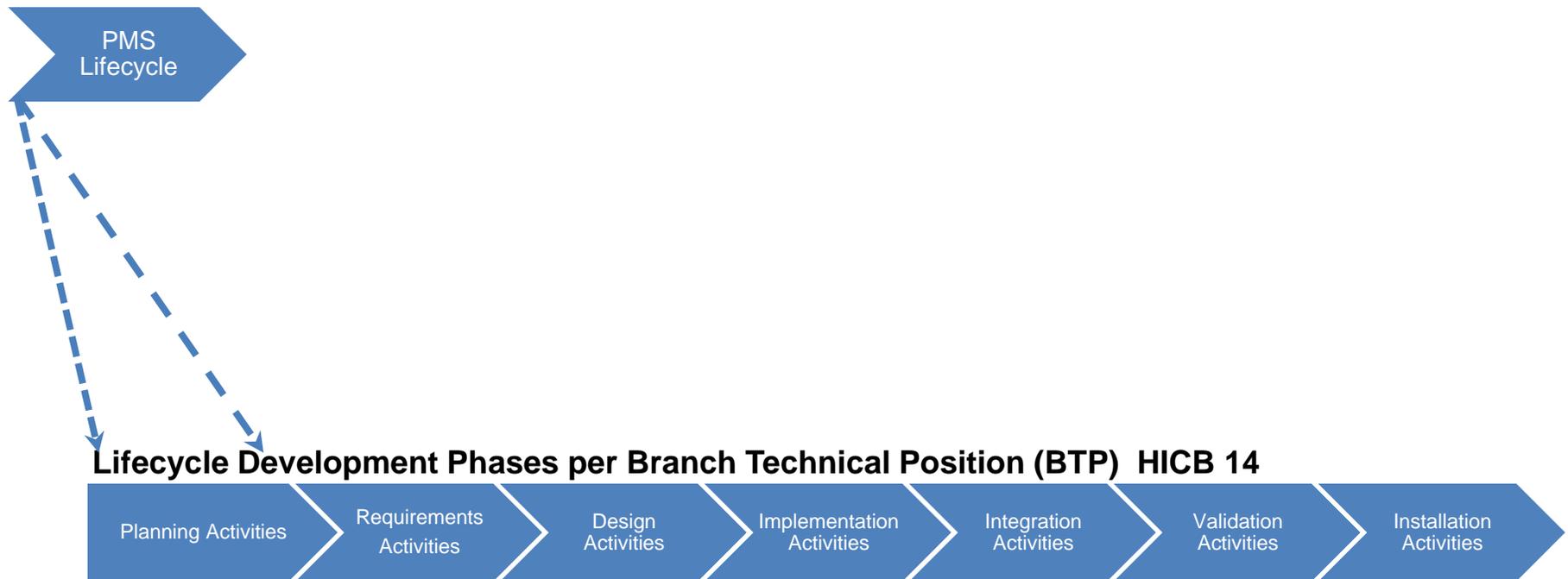
- Staff sent a letter to Westinghouse on March 24, 2009, during its review process, regarding technical issues identified in document reviews and audits.
  - WEC replied to Staff concerns on April 21, 2009
- The issues related to a lack of information for:
  - **Component Interface Module (CIM), the priority module for PMS**
  - **Diversity and Defense-in-Depth Analysis**
  - **DAS Development Documents**
  - **Testing Methodology**
  - Revised Technical Reports
  - **Computer Security Plan**

# Vertical Cross Section of DAC Review Process Related to IV&V



# Vertical Cross Section of DAC Review Process Related to IV&V

Protection and Safety Monitoring System Development



# PMS DAC Review Process Related to IV&V

## PMS Lifecycle Development Process Review Example

- The Software Independent Verification and Validation (IV&V) aspect of the PMS Design Requirements Phase illustrates the level of depth to which staff reviewed Westinghouse's detailed design material.
- The staff used the review methodologies and acceptance criteria presented in the regulations and guidance documents listed on the previous slides to validate the applicant's claim of phase completion related to DAC/ITAAC for the PMS
  - BTP HICB-14, Section B.3.1.10, Software Verification and Validation Plan
  - Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Rev. 0, September 1997) that endorsed
    - IEEE Std. 1012-1988, "IEEE Standard for Software Verification and Validation"
    - IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits"

# PMS DAC Review Process Related to IV&V

## PMS Lifecycle Development Process Review Example

- During the review of the AP1000 amendment, the staff discovered the following with regard to IV&V:
  - The applicant removed the references to several Tier 2\* documents, including WCAP-15927
  - WCAP-15927 was created as a response to a Request for Additional Information (RAI) in the original review to address additional conservative measures taken during the Common Q development process in addition to those already present in the Common Q Software Program Manual (SPM)
  - WCAP 15927 discussed how the application-specific AP1000 Common Q SLC development process would conduct IV&V activities

# PMS DAC Review Process Related to IV&V

## PMS Lifecycle Development Process Review Example

- Due to the additional commitments in WCAP-15927, the IV&V activities would be handled exclusively by the IV&V organization, thus satisfying 10 CFR 50 Appendix B, Criterion III – Design Control as it relates to IV&V
- Under the Common Q SPM either the design team (DT) or the V&V team (VT) could be responsible for testing during the phases of Common Q development

# PMS DAC Review Process Related to IV&V

The staff requested Westinghouse (WEC) respond to the question below:

- Westinghouse removed WCAP-15927, “Design Process for AP1000 Common Qualified Platform Safety Systems,” from its list of Tier 2\* documents without stating how it will still meet the IV&V requirements in its lifecycle development process for the PMS

# PMS DAC Review Process Related to IV&V

Westinghouse deleted Tier 2\* references in the AP1000 DCD

REVISION 15			REVISIONS 16 and 17		
Item	Exp. @ Full Power	Tier 2 Reference	Item	Exp. @ Full Power	Tier 2 Reference
WCAP-13383, "AP600 Instrumentation & Control H/W & S/W Design, Verification & Validation Process Report," Rev 1.	Yes	Chapter 7 Table 1.6-1	<del>WCAP-13383, "AP600 Instrumentation &amp; Control H/W &amp; S/W Design, Verification &amp; Validation Process Report," Rev 1.</del>	Yes	<del>Chapter 7 Table 1.6-1</del>
WCAP-14605, "Westinghouse Setpoint Methodology for Protection Systems, AP600," Rev 0	Yes	Chapter 7 Table 1.6-1	WCAP-14605, "Westinghouse Setpoint Methodology for Protection Systems, AP600," Rev 0	Yes	Chapter 7 Table 1.6-1
CENPD-396-P, Rev. 01, "Common Qualified Platform"	Yes	Chapter 7 Table 1.6-1	<del>CENPD-396-P, Rev. 01, WCAP-16097-P-A "Common Qualified Platform" Rev 1</del>	Yes	Chapter 7 Table 1.6-1
CE-CES-195, "Software Program Manual for Common Q Systems," Rev 01	Yes	Chapter 7 Table 1.6-1	<del>CE-CES-195, WCAP-16096-NP-A "Software Program Manual for Common Q Systems," Rev 01-A</del>	Yes	Chapter 7 Table 1.6-1
WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," Rev 0	Yes	Chapter 7 Table 1.6-1	<del>WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," Rev 0</del>	Yes	<del>Chapter 7 Table 1.6-1</del>
Verification and Validation	Yes	7.1.2.14	Verification and Validation	Yes	7.1.2.14
Hard-wired DAS manual actuation	No	7.7.1.11	Hard-wired DAS manual actuation	No	7.7.1.11

- This deletion triggered several questions from the staff

# PMS DAC Review Process Related to IV&V

**Westinghouse Response: July 7, 2008**

- The SPM for Common Q Systems is a Tier 2\* document that addresses these items requested in the original RAI.
- The NRC stated in it's SER for the Common Q Platform, that the Common Q SPM specifies plans for implementing a structured software life cycle process for application software and provides guidance for configuration management of commercial-grade hardware and previously developed software.
- The issue regarding module testing was subsequently closed in the NRC SER dated June 2001, Therefore the original request for docketed design process information is fulfilled by the SPM for Common Q Systems (WCAP-16096-NP-A) and NABU-DP-00014-GEN do not have to be Tier 2\* documents

# PMS DAC Review Process Related to IV&V

- Staff observed the response did not adequately answer the question posed
  - The Staff reviewed the Common Q SPM, particularly Exhibit 5-1, that allowed either the Design Team (DT) or the (VT) to perform testing on equipment developed by the Design Team for protection systems
  - This process did not meet 10 CFR 50 Appendix B, Criterion III - Design Control

*The design control measures shall provide for verifying or checking the adequacy of design, such as by the performance of design reviews, by the use of alternate or simplified calculational methods, or by the performance of a suitable testing program. **The verifying or checking process shall be performed by individuals or groups other than those who performed the original design...***
  - Revision 0 of WCAP-15927 provided this necessary measure, and its removal would allow a safety-related design process outside of regulations.

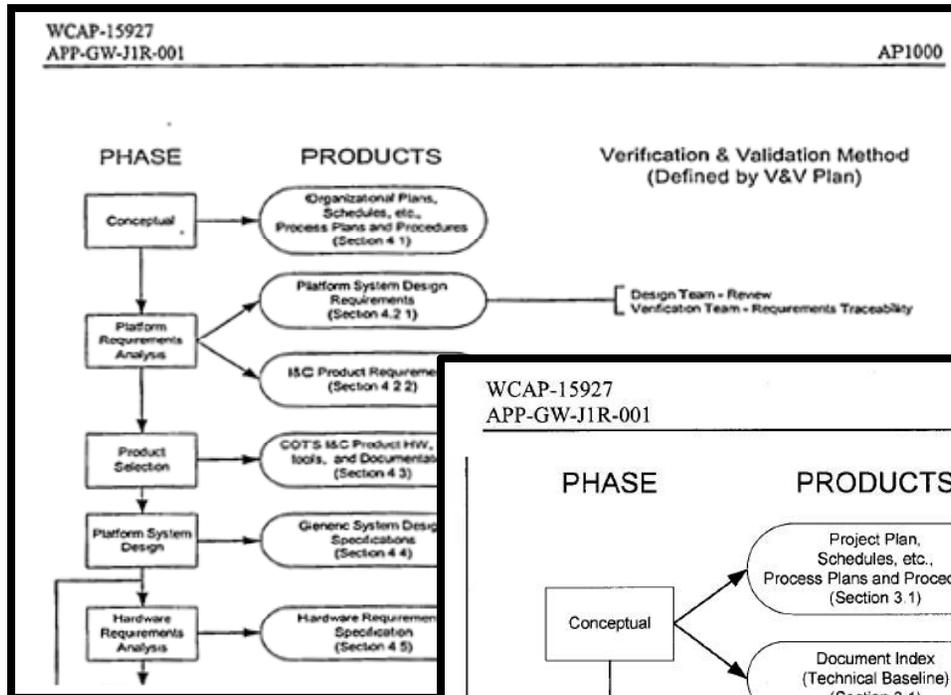
# PMS DAC Review Process Related to IV&V

- Information obtained from Westinghouse via phone calls led the staff to audit additional documentation, most notably its proprietary *Verification & Validation Process for the Common Q Safety Systems*, WNA-PV-00009-GEN to support its position that the WCAP-15927 document was no longer required.
  - The presented document stated WEC committed to follow IEEE 1012-1998, “IEEE Standard for Software Verification and Validation” until it deviated with the less conservative guidance within the Common Q SPM. However the staff noted the document was a V&V Process for generic Common Q equipment, not application specific equipment such as the AP1000.
  - IEEE 1012 requires Requirements Traceability Analysis (RTA) be conducted by the V&V Team as does Revision 0 of WCAP 15927
  - The staff reviewer noted the current document, Revision 3, had been issued in August 2008.
  - Upon presentation with the revision of the document in effect during certification, the text committed to follow IEEE 1012-1998 implicitly without regard for the SPM.

# PMS DAC Review Process Related to IV&V

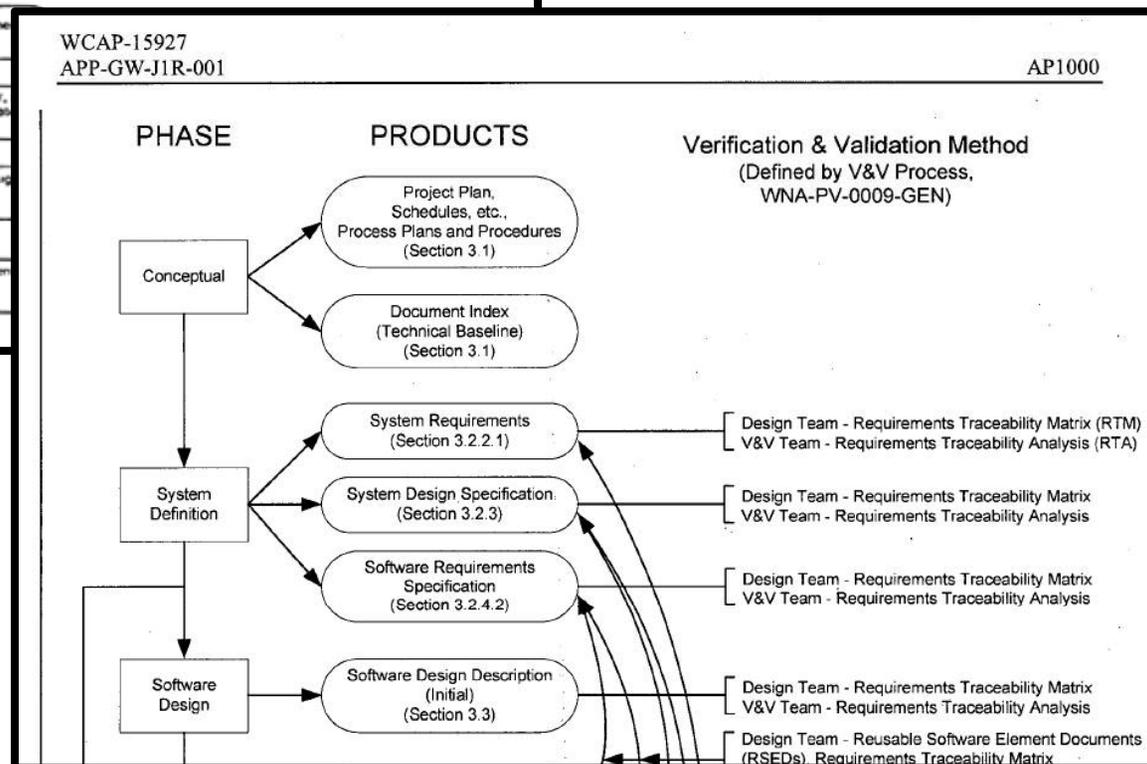
- Westinghouse responded by providing a draft of WCAP-15927, Revision 1, during the April 2009 audit. The document allowed the design team to conduct Requirements Traceability rather than the IV&V team.
  - The staff informed WEC that the document, in its current form, would not be accepted as a replacement for Revision 0 of the document
- Westinghouse modified their software IV&V procedure such that the functions of developing the Requirements Traceability Matrix (RTM) and Requirements Traceability Analysis (RTA) would be split out to the DT and VT respectively.
- Westinghouse docketed WCAP-15927, Revision 2, which displayed the necessary differentiation between the two organizations and their roles.

# PMS DAC Review Process Related to IV&V



WCAP 15927 Figure 3

Revision 0



Revision 2



# PMS DAC Review Conclusion

## (for 1<sup>st</sup> 2 phases of SLC development)

- Based upon the combination of the additional material reviewed by the staff, and the audits conducted, the staff reached the following conclusions:
  - The Design Requirements (Planning Activities) phase of PMS development process is considered complete provided that
    - The CIM Lifecycle Development Process remain as DAC in Tier 1 of the AP1000 DCD as the process described was insufficient for the staff to conclude it met regulations or satisfied associated guidance
  - The System Definition (Requirements Activities) phase of PMS is not complete
    - Based upon the results of three audits, the staff concluded WEC has additional technical and clarifying information it needs to provide to the staff before the staff may reach a determination of completion of the phase
    - The staff expects to see the System Definition phase added back into Tier 1 information within Revision 18 of the AP1000 DCD

# PMS DAC Review Conclusion

WEC committed to add Item 14 to Tier 1 ITAAC

Tier 1, Chapter 2, Table 2.5.2.-8 Inspections, Tests, Analyses, and Acceptance Criteria		
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
14. The Component Interface Module (CIM) is developed using a planned design process which provides for specific design documentation and reviews.	An inspection and or an audit will be performed of the processes used to design the hardware, development software, qualification and testing.	A Safety Evaluation Report exists and concludes that CIM meets the below listed life cycle stages and is approved for use in the AP1000 safety related PMS. Life cycle stages: a. Design requirements phase, may be referred to as conceptual or project definition phase b. System definition phase c. H/W and S/W development phase, consisting of hardware and software design and implementation d. System integration and test phase e. Installation phase

# Future Efforts

- The same level of effort will be applied to future technical and process information received related to amended Design Certifications and licensing reviews
  - A more robust CIM Development Process document(s) is expected
  - Westinghouse will address the staff concerns from the April 2010 audit to meet regulations and satisfy guidance related to the System Definition Phase
    - If documents regarding the CIM and System Definition phases are submitted, the staff will review these.
    - The staff will perform the same type of reviews as conducted in March and April 2010 audits to verify adequacy of the Westinghouse engineering documents.
- Technical agency experts from I&C, Region II, and other technical experts will continue to support the review, audit/inspection, process and resolution/closeout effort

# DAC Review Conclusions

- NRC staff performs an in-depth evaluation of vendor engineering documents to verify the resolution/closeout of DAC/ITAAC material and will address non-compliance as necessary.
- Acceptance criteria, review tools, technical report review and level of effort for inspections are similar to those used in audits during design certification and license reviews
  - Inspection activities are similar to what occurred during audit activities
  - Little differentiation between DAC and ITAAC (some ITAAC are also heavily design oriented)
- Technical agency experts conducting licensing reviews will also be involved in DAC/ITAAC inspections

**Questions ???**

# Auxiliary Slides

## Index

- Possible format of I&C DAC/ITAAC Information in Tier 1 material within Revision 18 of the AP1000 DCD, based upon WEC commitments, via RAI responses (2 slides)
- Example of Section 3.2.1 of NUREG/CR 6101
- Example of two points within DI&C ISG-04 HICRc
- Tier 2\* Information
- Level of Effort and Design Understanding Graph
- Licensing and Design Documents within and beyond FSAR
- Full Text of Staff RAI to Westinghouse regarding IV&V
- Full Text of Westinghouse response to Staff RAI regarding IV&V

# Possible Format of Text-Based Portion of ITAAC Within Tier 1 Information related to PMS

## POSSIBLE FORMAT OF REVISION 18 \*

### Design Description 11

The PMS hardware (H/W) and software (S/W) is developed using a planned design process which provides for specific design documentation and reviews during the following lifecycle stages

- a.) Design Requirements - **Complete**
- b.) System Definition
- c.) H/W and S/W Development & Implementation
- d.) System Integration & Test
- e.) Installation

\*Based upon commitments made by Westinghouse in several RAI responses

# Possible Format of Table-Based Portion of ITAAC Within Tier 1 Information related to PMS

<b>POSSIBLE FORMAT OF REVISION 18 OF AP1000 DCD*</b>		
<b>Design Commitment 11</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
The PMS H/W and S/W is developed...	Inspection will be performed of the process used to design the H/W & S/W	A report exists and concludes...
b.) System Definition		Specification of functional requirements
c.) H/W and S/W Development & Implementation		Documentation and review of H/W and S/W
d.) System Integration & Test		Performance of system tests and documentation of test results
e.) Installation		Performance of installation tests and inspections

\*Based upon commitments made by Westinghouse in several RAI responses

# Safety-Related Communications

- For example, BTP HICB- 7-14 describes the material within an acceptable software lifecycle development process as does IEEE Std. 1074, as endorsed by RG 1.173. Additionally, NUREG/CR 6101 and DI&C ISG-04 describe detailed metrics one may use to judge the Planning or Requirements Activities as satisfactorily complete.
  - Section 3.2.1 of NUREG/CR 6101 describes items to check for and validate for a Software Requirements Specification
    - Point 11 – Software Interface Requirements – Define all communication interfaces between systems and why they are acceptable.
  - DI&C ISG-04 Highly Integrated Control Rooms-Communications Issues (HICRc) contains acceptance criteria related to data communications

# Example of Section 3.2.1 of NUREG/CR 6101

## 3.2.1. Software Requirements Specification

The SRS is required for a safety-critical application, to make sure that all safety-related system requirements are made known to the software developers. These requirements come from the overall application system design, and reflect the requirements placed on the software by the application system. In a reactor protection system, this means that the protection

11. **Software Interface Requirements.** If the software system will communicate with any other application software system, define all the interfaces between the systems. This communication may be in terms of subroutine calls, remote procedure calls, communication messages, or some other means. All such are referred to as “messages” here.

–For each message, describe the source and destination of the message, the message contents and format, the meaning of the message, expected return messages, transmission method and medium, error conditions, expected frequency and size, and a reasonable upper limit to frequency and size. An upper limit to frequency, for example, could be a frequency that is exceeded less than 0.01% of the time.

–Interactions between the application program and the operating system are not usually considered to be interfaces that must be defined here. There may be rare exceptions, however, in particular cases.

The following aspects of communication system interfaces should be considered if they apply to the application (Redmill 1988):

- \* Handshaking
- \* Error checks
- \* Input and output communication ports
- \* Communication protocols and procedures
- \* Interrupts
- \* Exception handling and error recovery
- \* Message formats
- \* Message throughput

See Preckshot 1992a for more information on communication systems.

# Example of DI&C HICRc Acceptance Criteria

## **STAFF POSITION**

Bidirectional communications among safety divisions and between safety and non-safety equipment is acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. Systems which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety equipment should adhere to the guidance described in the remainder of this section. Adherence to each point should be demonstrated by the applicant and verified by the reviewer. This verification should include detailed review of the system configuration and software specifications, and may also involve a review of selected software code.

1. A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.
2. The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

# Tier 2\* Information

## AP1000 Design Control Document - Introduction

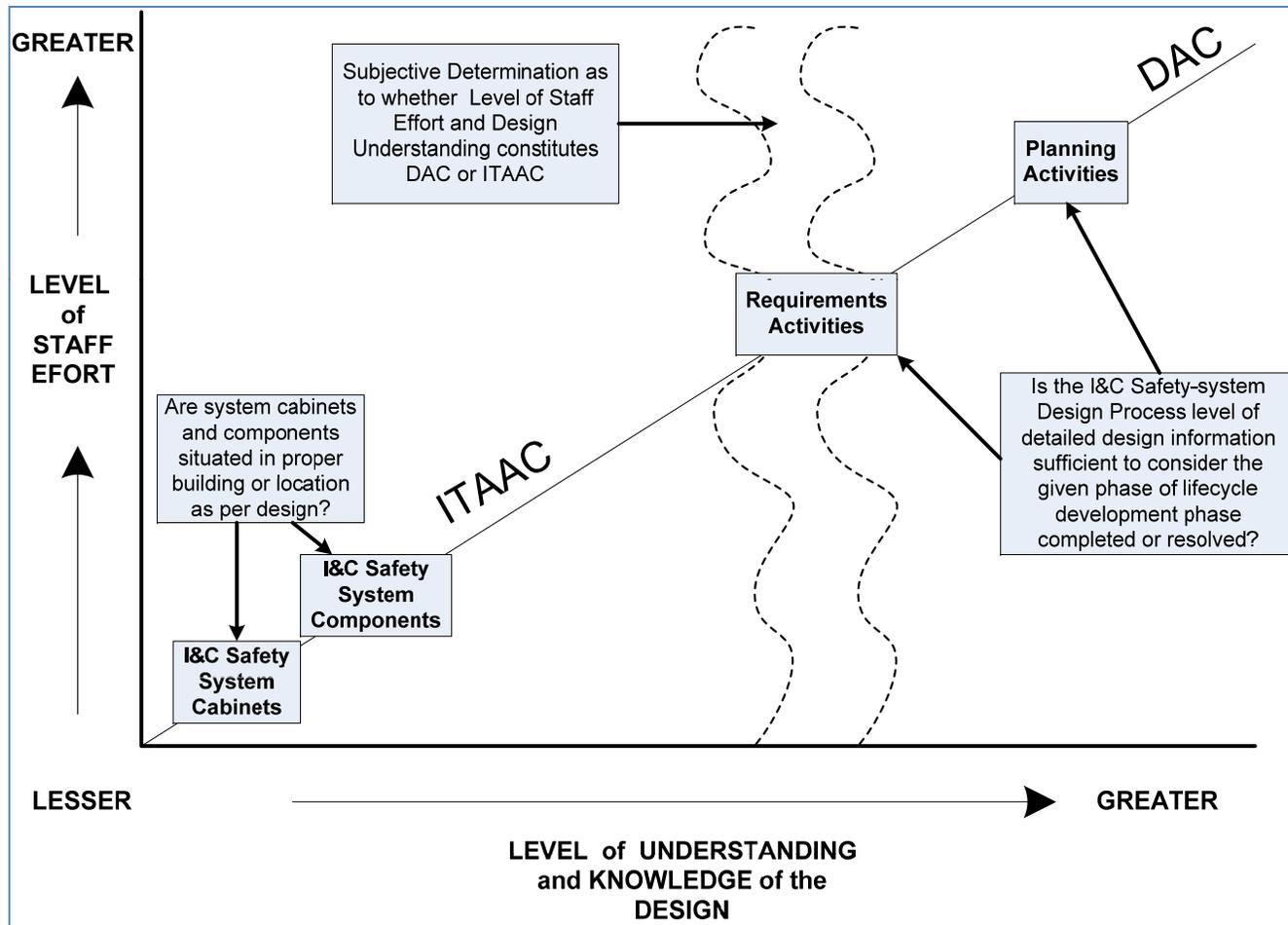
### 3.5 Plant-Specific Changes to Designated Information in the Tier 2 Information

*Tier 2\** means the portion of the Tier 2 information, designated as such in the AP1000 design control document, which is subject to the change process in Section VIII of the AP1000 design certification rule. This designation expires for some Tier 2\* information under Section VIII of the AP1000 design certification rule.

An applicant who references the AP1000 design certification rule may not depart from Tier 2\* information, which is designated with italicized text or brackets and an asterisk in the AP1000 design control document, without NRC approval. The departure will not be considered a resolved issue, within the meaning of Section VI of the AP1000 design certification rule and 10 CFR 52.63(a)(4).

The AP1000 Tier 2\* information, summarized in Table 1-1 of this introduction, is designated with italicized text in the Tier 2 Information. Certain figures that are indicated to be Tier 2\* may contain information beyond that that is considered to be Tier 2\*. A review of the text referencing **the figure may be necessary to determine what information on the figure is considered to be Tier 2\***. The AP1000 Tier 2\* information for which the Tier 2\* designation expires when the COL holder first achieves 100% power operation is indicated in Table 1-1 of this introduction.

# DAC/ITAAC Level of Effort and Design Understanding Graph



# Licensing and Design Documents within and beyond FSAR

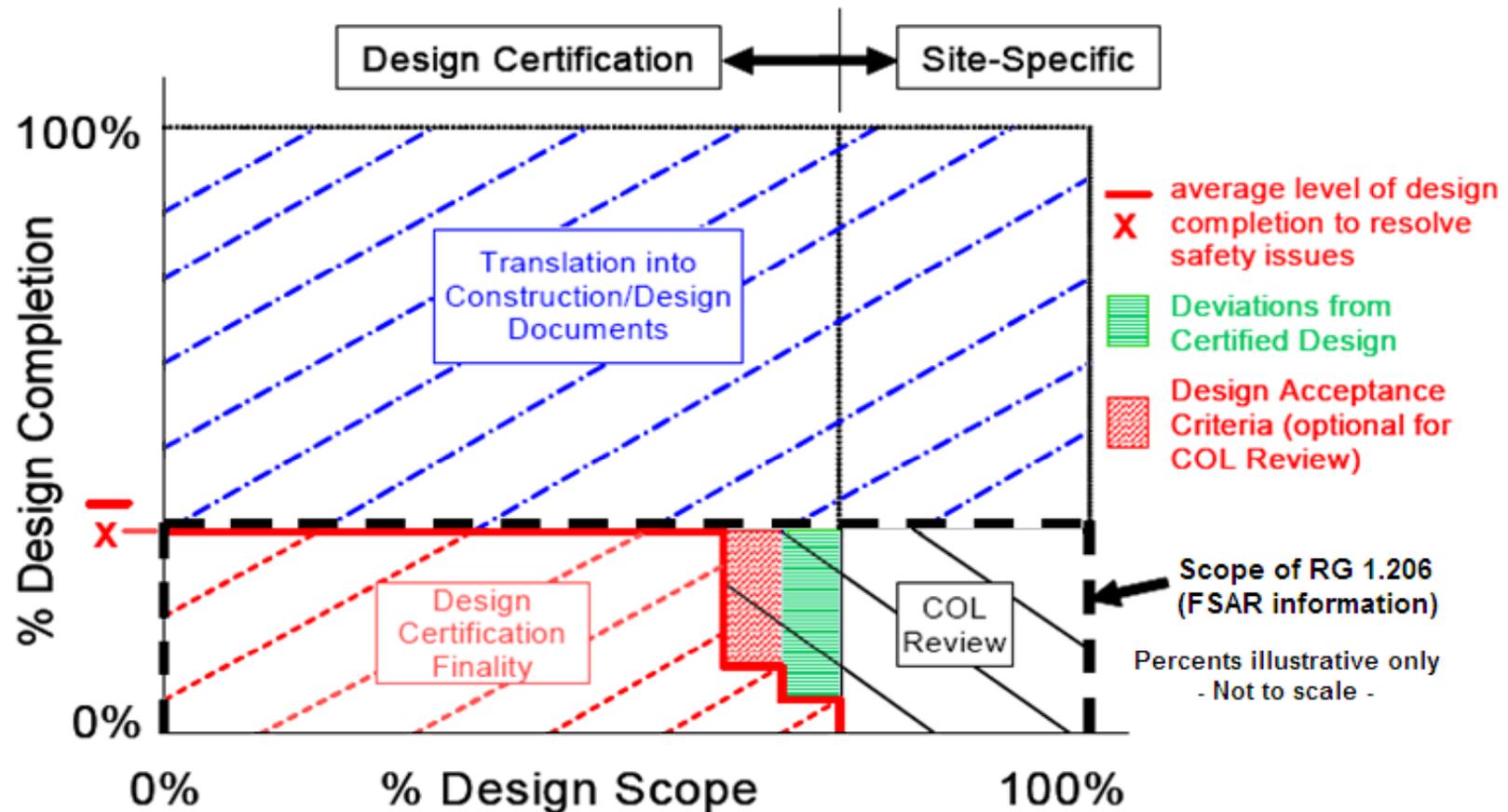


Figure 1 (from RG 1.206, Section B, “Discussion”): Combined License Referencing a Certified Design

# PMS DAC Review Process Related to IV&V

The staff requested Westinghouse (WEC) respond to the RAI listed below: (full text)

- Westinghouse has requested to remove the reference to WCAP-15927, “Design Process for AP1000 Common Qualified Platform Safety Systems,” which was submitted in addition to the Software Program Manual WCAP-16096-NP-A, Revision 1A (previously designated as CES-195, Revision 1) to resolve Requests for Additional Information 420.001 and 420.023, posed during the development and certification of the original AP1000 final safety evaluation report. Demonstrate what measures will be taken to ensure information contained in this report are not removed. If another document covers the same information but is not currently on the docket, submit that document on the docket.

# PMS DAC Review Process

- **Westinghouse Response: July 7, 2008 (full text)**

RAI 420.023 requested a description of a formal design implementation process with a phased inspection, test, analysis and acceptance criteria (ITAAC) for AP1000 specific Common Q system design development. The description of the development plan should include details of the hardware and software management plan, the configuration plan, and the verification and validation plan. The detailed description should be non-proprietary. The new document should be part of AP1000 Tier 2 Information Requiring NRC Approval for Change (Tier 2\*). The Software Program Manual for Common Q Systems, WCAP-16096-NP-A (Reference 1), is a Tier 2\* document that addresses these items requested in RAI-420.023. The NRC stated in it's SER for the Common Q Platform, ML003740165 (Reference 2), "CENP's 'Software Program Manual for Common Q Systems' (SPM) specifies plans for implementing a structured software life cycle process for application software and provides guidance for configuration management of commercial-grade hardware and previously developed software." "The staff finds the software program manual acceptable dependent upon the resolution of an open item related to the scope of module testing. Licensees using the Common Q platform for plant-specific applications will be required to implement the application software in accordance with CENP's software program manual."

The issue regarding module testing was subsequently closed in the NRC SER dated June 2001, ML011690170 (Reference 3), (see RAI response RAI-SRP 7.1-ICE-29). Therefore the original request for docketed design process information is fulfilled by the Software Program Manual for Common Q Systems (WCAP-16096-NP-A), and NABU-DP-00014-GEN (Reference 4) does not have to be Tier 2\*.

# Review & Implementation Process for ESBWR Instrumentation and Controls Design Acceptance Criteria – Single Failure Criterion

Instrumentation, Controls & Electrical Engineering

Branch 2

Division of Engineering

Office of New Reactors

# Example of DAC from ESBWR

- The staff selected this example DAC in order to support the Committee and explain in detail
  - the scope
  - the level of detail
  - the depth and breadthof both the DCD and the Staff review
- The single failure criterion is an integral part of the overall safe plant design

# Outline

## Example of DAC from ESBWR

- Definition
- Safety Issue, Significance, and Finding
- Requirements and Guidance
- Tier 1 and 2 Information
- Staff Review of DCD
- Acceptability and Quality of DAC
- DAC Inspection

# Definition

*Single Failure Criterion From IEEE 603-1991*

The safety systems shall perform all required safety functions for a design basis even in the presence of the following:

- Any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable failures.
- All failures caused by the single failure.
- All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function.

The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function.

# Safety Issue, Significance and Finding

- Safety Issue
  - Safety I&C system design must be designed to achieve high functional reliability and thus to cope with a single failure.
- Safety Significance
  - Protection against a single failure ensures high functional reliability of the safety system through redundancy and independence.
- Safety Finding – as determined by the staff and approved by the ACRS
  - ESBWR I&C system is designed with sufficient redundancy and independence.
  - The DCD sufficiently describes the design details and the design complies with the single failure criterion requirement.
  - In addition, the DCD includes a detailed, well-structured methodology/process as well as a set of DAC and ITAAC ensuring a high-quality translation of the licensing basis into the detailed implementation that are found to be acceptable to the staff.

# Requirements & Guidance

## Requirements

- 10 CFR 50 Appendix A (e.g. GDC 21, 23)
- 10 CFR 50.55a(h)
  - IEEE 603-1991 Clause 5.1

## Guidance

- NUREG-0800, “Standard Review Plan”
- IEEE 7-4.3.2-2003 Section 5.1
- Regulatory Guide 1.53, “Application of the Single-Failure Criterion to Safety Systems”
- IEEE 379-2000, “Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”

# Single Failure Criterion Integrated in Overall DCD

- All safety systems (including I&C) are required to comply with the single failure design criterion
  - GDC17, Electric Power Systems
  - GDC 34, Residual Heat Removal
  - GDC 35, Emergency Cool Cooling
  - GDC 38, Containment Heat Removal
  - GDC 41, Containment Atmosphere Clean-up
  - GDG 44, Cooling Water
- One of 15 Clauses in Section 5, “Safety System Criteria” of IEEE 603-1991
- Evident throughout the Lifecycle Process

# Single Failure Criterion Integrated in Overall DCD

- Redundancy and Independence within
  - Division
  - System
  - Logic, etc.
  - Lifecycle Process
    - Each safety system implements
    - DAC/ITAAC are resolved
- Single Failure Criterion was referenced over 250 times for the Tier 1 and 2 for I&C

# Tier 1: Safety System Applicability

Table 2.2.15-1  
IEEE Std. 603 Criterion System Applicability Matrix <sup>(1)(2)</sup>

Software projects/Project		RTIF-NMS Platform							SSL/ESF Platform							ICP Platform							
		RTIF							NMS							VBIF	A TWS/ SLC	HP CRD IBF	ICS DPV IF				
Table 2.2.15-2, Item No.	IEEE Std. 603 Criterion	RTIF (2.2.10)	RPS (2.2.7)	LD&S MSIV (2.2.12) [Note (4)]	CMS-SPTM (2.15.7)	NBS (2.1.2)	CRD (2.2.2)	NMS (2.2.5)	SSL/ESF (2.2.13)	LD&S non-MSIV (2.2.12) [Note (3)]	PRMS (2.3.1)	CMS non-SPTM (2.15.7) [Note (4)]	NBS (2.1.2)(A)DS (N/A)	GDCS (2.4.2)	ICS (2.4.1)	SLC (2.2.4)	CBVS (2.16.2.2, 2.16.2.3) [Note (5)]	CRD (2.2.2)	VB Isolation Function (2.15.1)	A TWS/SLC (2.2.14)	HP CRD Isolation Bypass Function (2.2.16)	ICS DPV Isolation Function (2.4.1)	
1	4.1	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R	R	R	R
2	4.4	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R	R	R	R
3	5.1	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R	R	R	R
5.2																							

# Example DAC Tier 1 DCD

**Table 2.2.15-2 ITAAC for IEEE Std. 603 Compliance Confirmation**

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
<p>8a. Criterion 5.1, Single-failure criterion: The software project's design bases show compliance with the single-failure criterion.*</p>	<p>Inspection of the software project's design phase summary BRR show that a Failures Mode and Effects Analysis (FMEA) have been completed. {{Design Acceptance Criteria}}</p>	<p>The software project design phase summary BRR show that a FMEA has been completed and show the software project's safety-related functions required for design basis events can be performed in the presence of:</p> <ul style="list-style-type: none"> <li>• Single detectable failures within safety-related systems concurrent with identifiable but non-detectable failures;</li> <li>• Failures caused by the single failure; and</li> <li>• Failures and spurious system actions that cause or are caused by the Design Basis Event (DBE) requiring the safety-related functions.</li> </ul> <p>{{Design Acceptance Criteria}}</p>

**\*Accompanying ITAAC (8b) for confirmation of as-built software project**

# Baseline Review Record

## Software Project Lifecycle Phase Summary BRR

- Reports document compliance with IEEE 603-1991
  - at the conclusion of each software life-cycle phase baseline as documented by the life-cycle phase Summary BRR
  - for each platform and network segment

# Tier 1 DCD Information

- “Demonstration of compliance with IEEE 603 means the Q-DCIS documentation includes design bases that make appropriate reference to IEEE 603 design criteria and that the resulting as-built equipment has been inspected, tested, or analyzed to show that the Q-DCIS will be capable of performing in accordance with the design bases.”
- “The choice of whether an inspection, test or analysis is required to close a particular ITAAC is defined in the documentation associated with DAC/ITAAC closure report for the software projects in response to ITAAC defined in Section 3.2 Software Development.”

# Tier 2 DCD Information

- Compliance with Single Failure Criterion

ESBWR

26A6642AW Rev. 08

Design Control Document/Tier 2

Table 7.1-2  
I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																						
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM					
		RTIF							NMS															
IEEE Std. 603 Section	Functions (H)	RTIF	RPS	LD&IS (MSIV Only) (H)	CMS (Includes SPTM) (H)	NBS (H)	CRD (H)	NMS (H)	SSLC/ESF (H)	LD&IS (Non-MSIV) (H)	PRMS	CM3 (H)	NBS (Includes ADS) (H)	GDCS	ICS	SLC (H)	CBVs (H)	CRD (H)	VBIF	ATWS / SLC (H) (H)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function		
4.12	Special design basis	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	<a href="#">7.1.6.6.1.1</a>
5.1	Single failure criterion	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2
5.2	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.2.3.3.1	7.1.6.6.1.3 7.2.1.3.1 7.3.3.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.2.2.3.1	7.1.6.6.1.3 7.3.5.3.1 7.4.3.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.5.3.3.1	7.1.6.6.1.3 7.5.2.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.1.2.3.1	7.1.6.6.1.3 7.4.4.3.1	7.1.6.6.1.3 7.4.1.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.6.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3	<a href="#">7.1.6.6.1.3</a>	

- In 7 safety platforms, 19 safety systems individually implement the single failure criterion; providing an overall plant design that can cope with a single failure.

# Tier 2 Information

Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	Q-DCIS																			N-DCIS						
	RTIF - NMS Platform							SSLC/ESF Platform												Independent Control Platform			Network Segments			
	RTIF						NMS																			
	RTIF	RPS	LD&IS (MSIV Only) <sup>(6)</sup>	CMS (Includes SPTM) <sup>(6)</sup>	NBS <sup>(6)</sup>	CRD <sup>(6)</sup>	NMS	SSLC/ESF <sup>(6)</sup>	LD&IS (non-MSIV) <sup>(1)(6)</sup>	PRMS	CMS <sup>(6)</sup>	NBS (Includes ADS) <sup>(6)</sup>	GDCS	ICS	SLC <sup>(6)</sup>	CBVS <sup>(2)</sup>	CRD <sup>(6)(e)</sup>	VBIF	ATWS/SLC <sup>(6)(e)</sup>	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF	
50.55a(j)(1)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.55a(h)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X					
50.62							X	X						X					X			X	X	X		

## GDCs

20	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
21	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
23	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

# Tier 2 Information

## Regulatory Guide

26A6642AW Rev. 08

Design Control Document/Tier 2

**Table 7.1-1  
I&C Regulatory Requirements Applicability Matrix**

	Q-DCIS																N-DCIS										
	RTIF - NMS Platform						SSLC/ESF Platform										Independent Control Platform				Network Segments						
	RTIF					NMS																					
Criteria 800,	RTIF	RPS	LD&IS (MSIV Only) <sup>(6)</sup>	CMS (includes SPTM) <sup>(6)</sup>	NBS <sup>(6)</sup>	CRD <sup>(6)</sup>	NMS	SSLC/ESF <sup>(3)</sup>	LD&IS (non-MSIV) <sup>(1)(6)</sup>	PRMS	CMS <sup>(6)</sup>	NBS (includes ADS) <sup>(6)</sup>	GDCS	ICS	SLC <sup>(6)</sup>	CBVS <sup>(2)</sup>	CRD <sup>(5)(6)</sup>	VBIF	ATWS/SLC <sup>(4)</sup> (6)	HP CRD Isolation Bypass Function	<a href="#">ICS DPV Isolation Function</a>	GENE	PIP A/B	BOP	PCF		
								X	X	X	X																
	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X					
	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X					
	X	X	X					X	X			X	X	X		X		X	X	X	X	X					

# Tier 2 Information

Section 7.1.6.6.1.2 Single Failure Criterion  
(IEEE 603-1991, Clause 5.1)

Safety-related system designed into four  
physically and electrically isolated divisions

- Independence Section 7.1.2.1.1
- Redundancy Section 7.1.2.1.3

Failure Modes and Effects Analyses (FMEAs)  
confirm the detailed design implementation of  
the safety-related system to the single failure  
criterion as defined in the DCD.

# Single Failure Criterion Integrated in Overall DCD

Redundancy and Independence  
implemented within

- Q-DCIS Division Level
- Each Safety System Level
- Each Logic Level

Single Failure Criterion can be found and  
described over 250 times for the Tier 1  
and 2 for I&C

# Q-DCIS Level Example

Intra-divisional and safety to non-safety related fiber-optic cable communication paths are redundant

- Support reliability and diagnostic capability

No failure of any single hardware component, in any one division, can lead to an inadvertent trip.

Safety-related cabinets and chassis are power by redundant safety-related UPS

- Reliability and diagnostic capability

Communications between divisions of safety-related systems, no single communication or power failure that results in the loss of a safety-related function

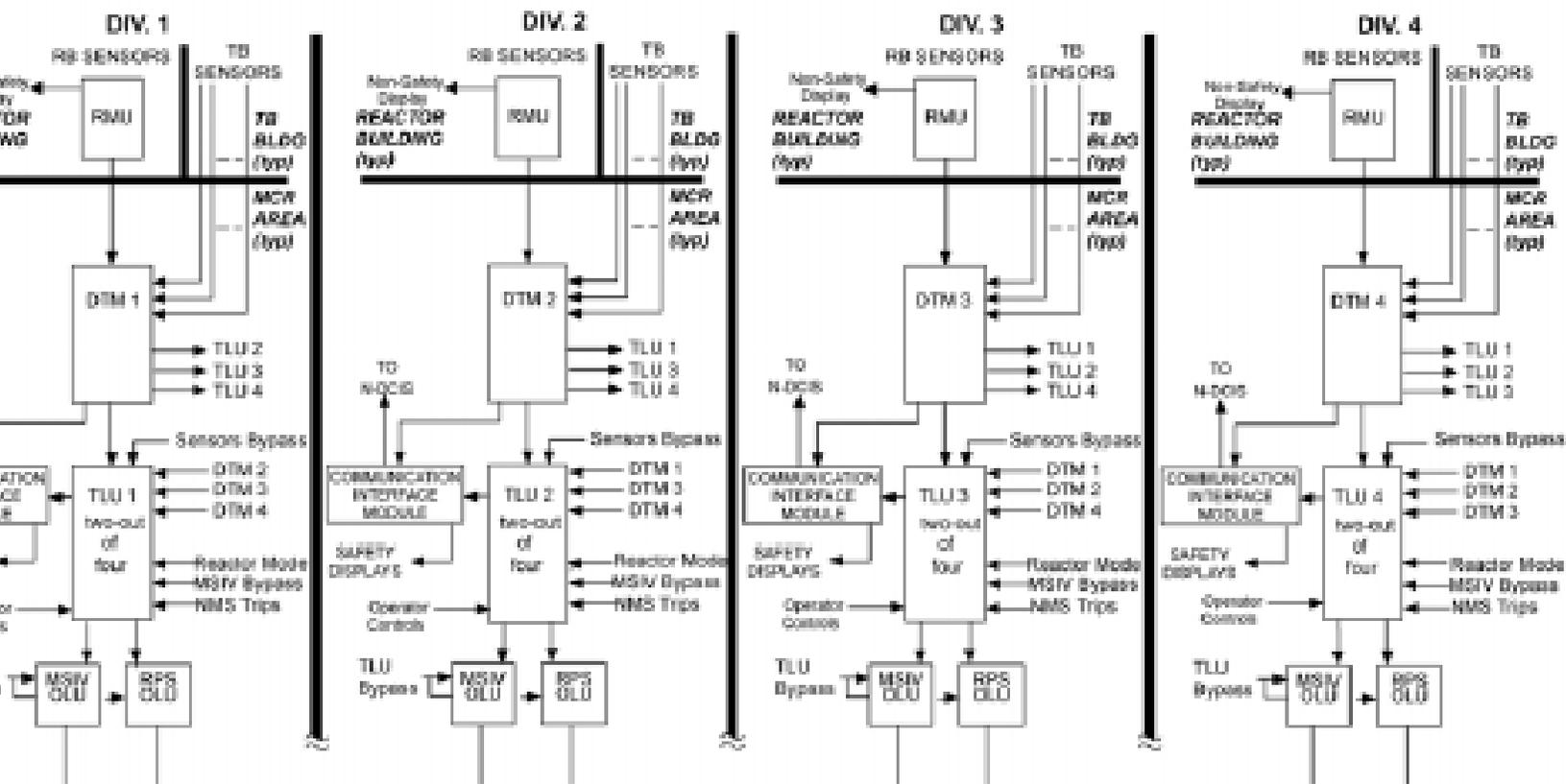
Safety-related systems perform their safety-related functions with 3 out of 4 safety-related divisions available, in the presence of a single failure.

# Reactor Protection System Level Example

RPS is organized into four physically and electrically-isolated divisions

- Utilize the principles of independence and redundancy for the single failure criterion as defined by
  - IEEE 379, Section 4
  - IEEE 603-1991, Clause 5.1
- Meets N-2 conditions
- Analyses complying with IEEE 379 will be used to confirm the safety-related system design conformance to the single failure criterion.

# RPS Simplified Functional Block Diagram



## Automatic Depressurization Actuation Logic Level

Each division of SSLC/ESF is configured such that all functions are implemented in triply redundant processors, to support the requirement that single divisional failures cannot result in inadvertently opening any ADS valve.

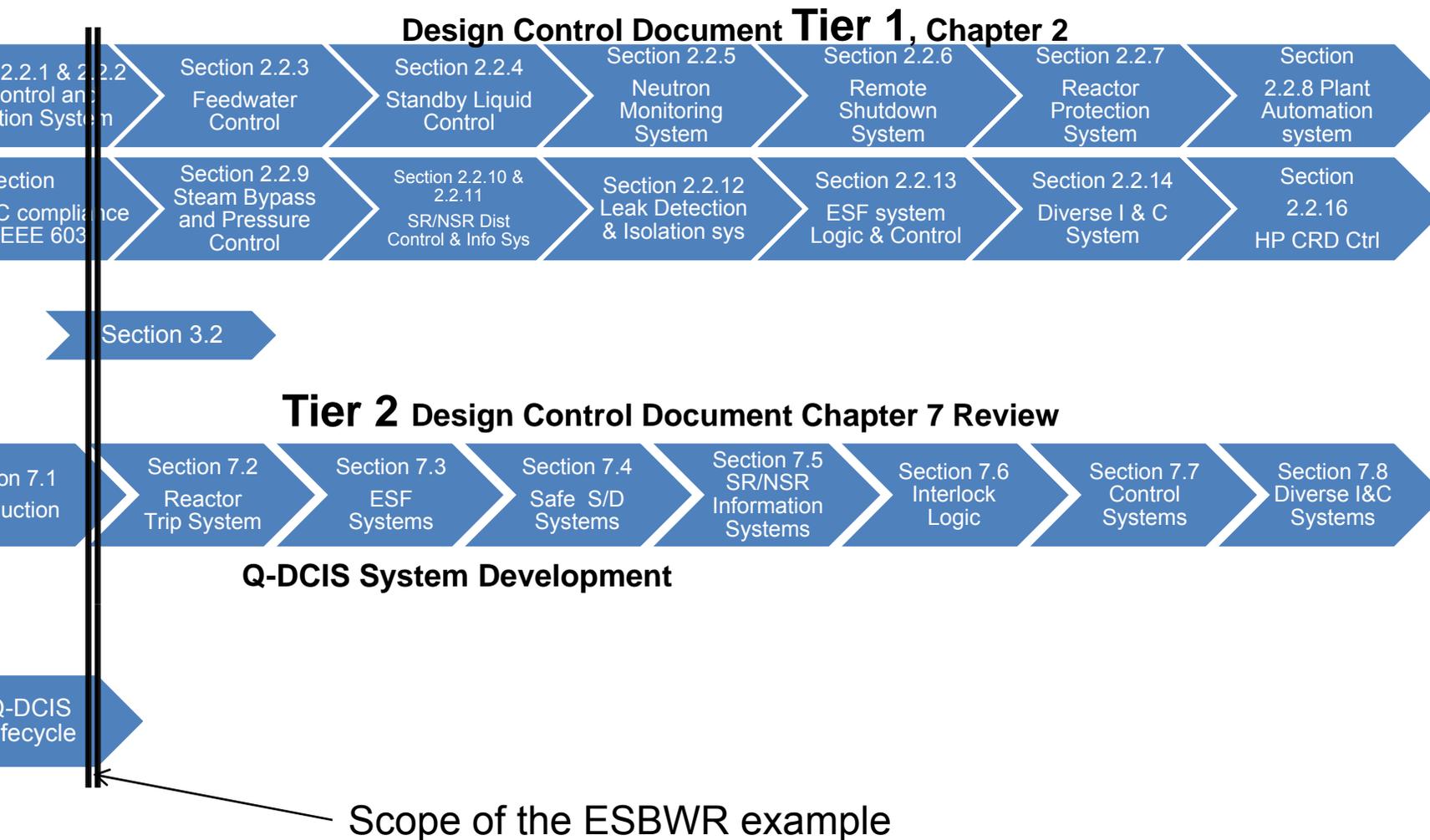
It is not possible to lose single failure inadvertent actuation protection by any operator or disable/test switch action.

No single failure of an

- ADS division logic
- SRV actuation pilot
- PDPV igniter circuit

can prevent successful system operation as long as any 2 out of 4 divisions of safety related power are available

# Vertical Cross Section of DAC Review Process Related to Single Failure Criterion



# Vertical Cross Section of DAC Review Process Related to Single Failure Criterion

DCIS System Development

Q-DCIS Lifecycle

In the 3 ½ years since the Office of New Reactors inception there have been:

- **13910** Man-hours worked on the ESBWR DCA
- **294** Requests for Additional Information presented to GEH

Lifecycle Development Phases per Branch Technical Position (BTP) HICB 14



# Tier 2 DCD Information – Lifecycle

The Single Failure Criterion is present throughout the lifecycle process.

Each safety system implements the lifecycle process.

DAC and ITAAC are also completed during the lifecycle process for each of the safety systems.

## Tier 2\* DCD Information – Lifecycle

Implementation Process - Lifecycle Process+

NEDE-33226 (Software Management Program Manual)++

NEDE-33245 (Software Quality Assurance Program Manual)++

- Planning Phase
- Requirements Phase
- Design Phase
- Implementation Phase
- Test Phase
- Installation Phase

– Also included in Topical Reports NEDO-33217, “ESBWR Man-machine Interface System and Human Factors Engineering Implementation” and NEDO-33295, “ESBWR Cyber Security Program Plan”

– All these documents are DCD Tier 2\* Information

# Overview of Staff Review of DCD

Information Reviewed

Tier 1 Information ( $\approx$ 250 pages)

– DAC/ITAAC

Tier 2 Information ( $\approx$ 500 pages)

Licensing Topical Reports ( $\approx$ 500 pages)

Conclusion – Staff found the I&C design in DCD for the ESBWR to have met the requirements of the single failure criterion.

# Staff Review of DCD

The DAC provides for a thorough implementation of the single failure criterion throughout the lifecycle process and in each of the safety systems.

## SBWR DAC Item 8a. Acceptance Criteria

The software project design phase summary Baseline Review Record (BRR) show that a FMEA has been completed.

BRR summarizes the detailed implementation of design and includes

- Configuration Management Report
- Software Safety Analysis
- Verification and Validation Report
- Secure Development and Operational Environment

# Acceptability and Quality of DAC

Staff found the I&C DAC to be adequate for verifying that the as-built I&C systems conform to the single failure requirements described in the DCD.

- Staff reviewed the specified DAC and found it to consist of adequate prescribed limits, parameters, procedures and attributes.
- Failure Modes and Effects Analysis (FMEA) is a systematic procedure for identifying the modes of failure and for evaluating their consequences.
- FMEA is to consider each major part of the system, how it may fail, and the effect of the failure.
- Integrated into the Software Development
- COL Information Item that requires the applicant/licensee shall notify the NRC staff at least six months prior to scheduled completion of each BRR and software plan designated as DAC.

# Conclusion

Staff found the I&C design for the ESBWR to have met the requirements of the single failure criterion.

# DI&C DAC Inspection

Division of Construction Inspection & Operational Programs  
Office of New Reactors

# DI&C DAC Inspection Objective

fundamentally:

*Verification that the DI&C design, as implemented,  
conforms to the licensing basis*

# DI&C DAC Inspection Overview

ITAAC inspection

Independent of licensing decision

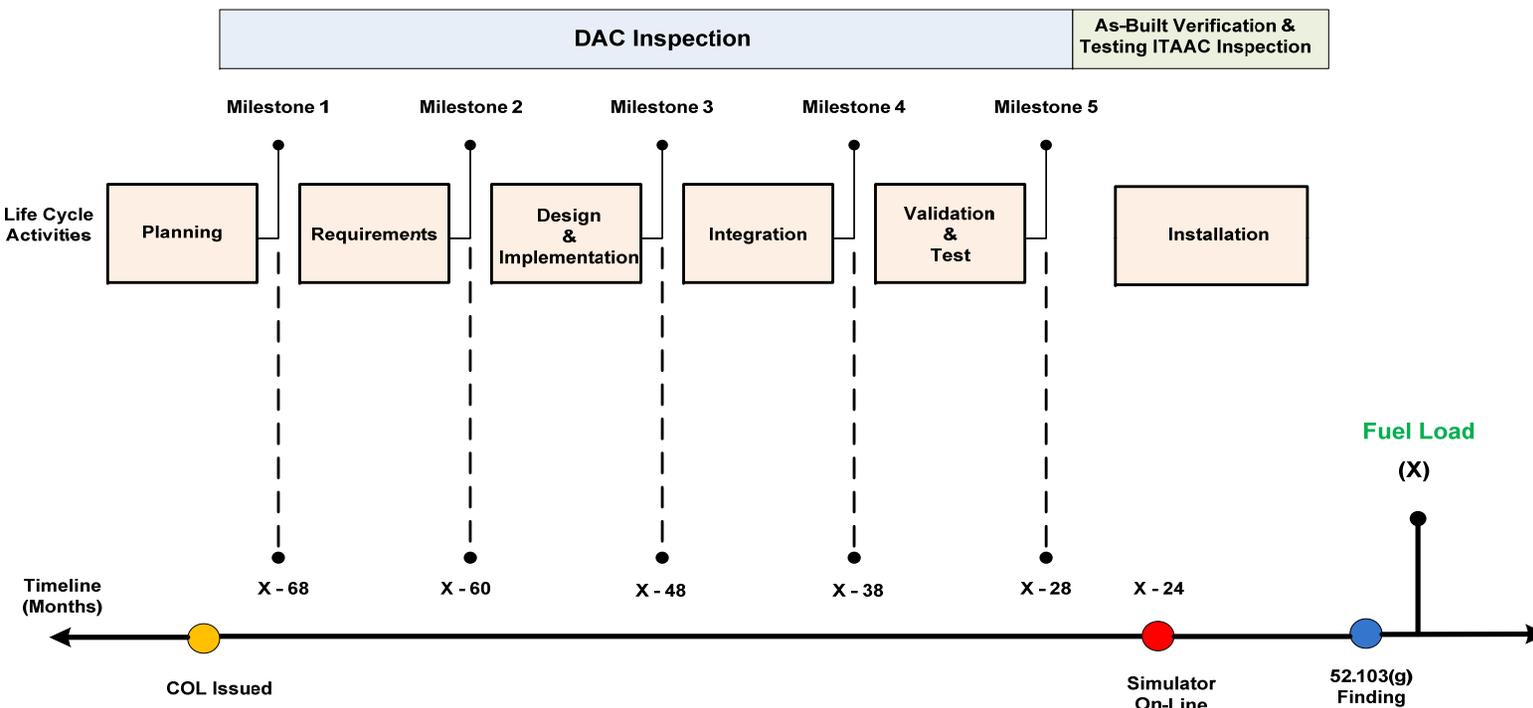
No impact on safety finding

Not an indication that ITAAC is complete

Focused on DI&C system/software fundamental design characteristics (attributes), development processes, and ITAAC (acceptance criteria)

Generally initiated and driven by applicant/licensee DI&C development milestones

# DI&C Inspection Timeline



**Digital I&C Development and  
Inspection Chronology  
(Notional)**

# Inspection Approach

All DI&C DAC are inspected

Synergistic team approach- regional I&C inspectors augmented by NRO DI&C technical staff

- same expertise engaged in licensing review
- team approach currently in use for South Texas DI&C DAC inspections

Inspection Procedure generally mirrors typical DI&C development life cycle w/ flexibility

Inspection activities are similar to audit activities

# ESBWR Example

T1 – ITAAC 2.2.15-2 (8a)

Design Commitment

Criterion 5.1, Single-failure criterion:  
The software project's design bases show compliance with the single failure criterion.

Inspection, Test, Analyses

Inspection of the software project's design phase summary BRR show that a Failures Mode and Effects Analysis (FMEA) have been completed.

{Design Acceptance Criteria}

# ESBWR Example (cont.)

T1 – ITAAC 2.2.15-2 (8a)

## Acceptance Criteria

The software project design phase summary BRR show that a FMEA has been completed and show the software project's safety-related functions required for design basis events can be performed in the presence of:

Single detectable failures within safety-related systems concurrent with identifiable but non-detectable failures;

Failures caused by the single failure; and

Failures and spurious system actions that cause or are caused by the Design Basis Event (DBE) requiring the safety-related functions.

{Design Acceptance Criteria}

# ESBWR Example (cont.)

Guidance is provided for the inspector in Appendix 3 (page A3-8) of the DI&C DAC IP (65001 Draft):

## c. Failure Analysis

A Failure Modes and Effects Analysis (FMEA) or other failure analysis should be performed to ensure that single failure requirements associated with system safety analyses and assumptions are confirmed. The FMEA should include system architecture to ensure that design principles of redundancy and independence have been incorporated and that single failure requirements are met. Verify the following from the FMEA or equivalent failure analysis:

1. All credible failure modes for the system/software were identified.
2. Impact (failure effect) on the system/software was evaluated.
3. Provisions to compensate for failure(s) are identified and included.

Guidance incorporated from NUREG/CR-6101 and IEEE-352

# ESBWR Example (companion ITAAC)

- T1 – ITAAC 2.2.15-2 (8b) (Standard ITAAC)
- Acceptance Criteria- Installation Phase report documents that as-built testing confirms the FMEA results
- RII inspectors will reconcile results of this ITAAC inspection with the previously documented results of the associated DAC inspection

# Documenting DAC Inspection

Governed by IMC 0613 (Documenting Part 52 Construction and Test Inspections)

Inspection Report is docketed

Inspection details are archived in CIPIMS database to support ITAAC closure process

# ITAAC Closure

Licensee completes DAC/ITAAC; NRC independently inspects

ITAAC Completion Letter (ICL) submitted to NRC

Staff reviews all ICLs, CIPIMS-archived information, supporting data related to the DAC/ITAAC

If no issues w/ ICL - staff issues *Federal Register* Notice (FRN)

If issues w/ ICL - enforcement per IMC 0613

FRN formally notifies licensee and public that the DAC/ITAAC is closed

# DAC Inspection Summary

Inspection program under development  
(lessons learned, process refinement, etc.)

Projected to conduct 3-4 South Texas  
DAC inspections in 2011

Plan to brief ACRS as key processes are  
implemented